

OTDK-dolgozat

2023

**DEBRECENI EGYETEM
GAZDASÁGTUDOMÁNYI KAR**



**DISZRUPTÍV PÉNZÜGYI MEGOLDÁSOK ÉS KOCKÁZATAIK
– MAGYARORSZÁGI ESETTANULMÁNYOK**

**DISRUPTIVE FINANCIAL SOLUTIONS AND THEIR RISKS
– HUNGARIAN CASE STUDIES**

Póta Cserne Panka

Konzulens: Dr. habil. Becsky-Nagy Patrícia

Kézirat lezárásának dátuma: 2021. október 25.

TARTALOMJEGYZÉK

1. BEVEZETÉS	1
2. TÉMAFELVETÉS	2
3. SZAKIRODALMI ÁTTEKINTÉS	4
3.1. A PÉNZÜGYI SEKTOR VÁLTOZÁSAINAK ÁLTALÁNOS BEMUTATÁSA A DIGITALIZÁCIÓ TÜKRÉBEN	4
3.2. DISZRUPTÍV TECHNOLOGIÁK ÉS ÚJSZERŰ ÜZLETI MODELLEK A FINTECH SEKTORBAN	6
3.3. MAGYAR HELYZETKÉP AZ ELEKTRONIKUS FIZETÉS VONATKOZÁSÁBAN.....	8
3.4. A DIGITÁLIS PÉNZÜGYI SZOLGÁLTATÁSOK MIATT FELMERÜLŐ KOCKÁZATOK	12
3.5. BIZTONSÁGI INTÉZKEDÉSEK ÉS MÓDSZEREK A PÉNZÜGYI KIBERKOCKÁZATOK ELHÁRÍTÁSÁRA.....	15
4. ANYAG ÉS MÓDSZER.....	19
5. EREDMÉNYEK ÉS AZOK ÉRTÉKELÉSE.....	21
5.1. A BARION PAYMENT ZRT. ESETTANULMÁNYA.....	22
5.2. A FINTECHX TECHNOLOGIES ZRT. ESETTANULMÁNYA	31
5.3. A SEON TECHNOLOGIES KFT. ESETTANULMÁNYA.....	38
5.4. A BANKMONITOR KFT. ESETTANULMÁNYA.....	43
6. KÖVETKEZTETÉSEK ÉS JAVASLATOK.....	49
7. ÖSSZEFOGLALÁS	52
SZAKIRODALMI JEGYZÉK.....	54

AZ INNOVÁCIÓS ÉS TECHNOLOGIAI MINISZTERIUM ÚNKP-21-2 KÓDSZÁMÚ ÚJ
NEMZETI KIVÁLÓSÁGI PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS
INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.

TÁBLÁZAT- ÉS ÁBRAJEGYZÉK

1. táblázat:	A PCI DSS szabvány céljai és követelményei	16
2. táblázat:	A Barion Payment Zrt. alapvető adatai	22
3. táblázat:	A Barionos fizetés bevezetése mellett- és ellen szóló érvek.....	29
4. táblázat:	A FinTechX Technologies Zrt alapvető adatai	32
5. táblázat:	A SEON Technologies Kft. alapvető adatai	39
6. táblázat:	A Bankmonitor Kft. alapvető adatai	43
7. táblázat:	A vizsgált vállalkozások esettanulmányainak rövid összegzése.....	50
1. ábra:	Az AFR folyamatábrája	9
2. ábra:	A FinTechX üzleti modelljének felépítése.....	37

1. BEVEZETÉS

Az utóbbi években egyre hangsúlyosabbá vált a 4. ipari forradalom részeként megszületett FinTech szektor. Ez az angol 'Financial Technology' kifejezés szóösszerántása, mely utal arra, hogy a pénzügyek egyre inkább összefonódnak a technológiai újításokkal. Az utóbbi években számos digitális pénzügyi megoldás, illetve újítás látott napvilágot, melyek fokozatosan fogják átszőni a mindennapjainkat. Az elektronikus fizetési lehetőségek használatának terjedése egyre inkább megfigyelhető Magyarországon is.

„Egy globális forradalomnak lehetünk szemtanúi, hiszen az innovatív megoldások világszerte, számos pénzügyi szolgáltatás területén – alternatív fizetési megoldások, biztosítás, hitelezés, költségkövetés, megtakarítások, pénzforgalmi rendszerek, pénzügyi menedzsment – nélkülözhetetlenné váltak (Droppa – Becsky-Nagy, 2019)”.

Napjainkban a pénzügyi szolgáltatások nyújtását erőteljesen meghatározza a platformizáció. A hatalmas platformok üzemeltetői közül a BigTech vállalkozások rendelkeznek a legnagyobb piaci erővel. Az elmúlt időszakban egyre többen nyújtanak közülük pénzügyi szolgáltatásokat is. Az ügyfelek platformon rögzített választásainak folyamatos nyomon követése lehetővé teszi számukra a személyre szabott szolgáltatásnyújtást. Az ipar 4.0 időszakában jelentek meg a FinTech cégek, melynek hatására döbbenetes ütemben kezdtek el terjedni a pénzügyi technológiai fejlesztések, amely a szektor hatékonyságát is növelte. A szektor új szereplői gyakran nagyszámú kockázati tőkét is kapnak a sikeres működésük érdekében. A hagyományos – készpénz alapú – fizetést is egyre inkább kiszorítják a különböző elektronikus fizetési módok. A bankkártya használat volt az első alternatív fizetési opció, ma azonban már számos lehetőség érhető el mind a kereskedők, mint a vásárlók szemszögéből. Magyarországon az azonnali fizetés bevezetése óta – a vírushelyzet kényszerítő hatását figyelembe véve – egyre népszerűbbek az elektronikus fizetési módok. A hazai és a külföldi FinTech szektorban is az adatelemzés és az üzleti intelligencia területe a leghangsúlyosabb, ezeken a területen tevékenykednek legmagasabb számban a FinTech cégek.

A PSD2 EU-s szabályozás megnyitotta a kapukat a nyílt bankolás felé, melynek keretében a bankok az ügyfelek előzetes engedélyét követően kötelesek harmadik feles – engedéllyel rendelkező – szolgáltatók számára kiadni az ügyfelek pénzügyi adatait. Az adatok sok szereplőn futhatnak keresztül, gyakran felhőalapú megoldásokat is alkalmaznak a szolgáltatók, ám ez a fajta hálózatosodás negatív hatást is kiválthat, hiszen így több fajta támadási felület áll az adathalászkok rendelkezésére. Az újszerű digitális pénzügyi szolgáltatások igénybe vevőinek adatait tehát nagy odafigyeléssel kell kezelni, hogy a visszaélések kiküszöbölhetőek legyenek.

2. TÉMAFELVETÉS

A kutatási téma aktualitását az adja, hogy a pénzügyek területét felforgató digitalizáció és a diszruptív technológiák begyűrűzése a pénzügyi szolgáltatásokba átformálta a hagyományos pénzügyi szektort. Megnövekedett a szereplők közötti verseny, az új belépők innovatív szemléletmódja pedig fejlesztésre ösztökélte az inkumbenseket is. A pénzügyek területén elterjedt innovációk révén felgyorsult az adatfeldolgozás és hatékonyabb lett a szolgáltatásnyújtás. A pénzügyi szolgáltatási folyamatok során az adatok sok szereplőn futhatnak keresztül, azonban ez a fajta hálózatosodás negatív hatást is kiválthat, hiszen így több fajta támadási felület áll az adathalászok rendelkezésére. Az elektronikus fizetési megoldások a digitális térben zajlanak, így az adatáramlás során kiberkockázati tényezők is közre játszhatnak. Az ügyféladatok védelme, a pénzügyi piac normális működésének fenntartása és az érzékeny adatokkal dolgozó szolgáltatók megfelelő felügyelete érdekében elengedhetetlen bizonyos szabályozások bevezetése.

A kutatásom célja, hogy kvalitatív módszereket, esettanulmányokat felhasználva feltárjam, hogy a digitális pénzügyi szolgáltatók hogyan változtatják meg a fizetési megoldások piacát, illetve milyen kockázatokat jelentenek a fizetési forgalom biztonságos lebonyolítására, valamint mennyire biztosított az új megoldások közötti átjárhatóság. A digitális pénzügyi szolgáltatásoknak csupán egy része a fizetési szolgáltatások területe, kutatásaim során a pénzügyi infrastruktúra szolgáltatókat és a hálózatosodásból eredő kockázatokat is górcső alá veszem.

A téma újszerűségéből, az iparágban meglévő bizonytalanságokból és annak dinamikus változásából, illetve a rendelkezésre álló hazai és nemzetközi adatok mennyiségének limitáltságából kifolyólag a kutatás eredményessége érdekében kvalitatív módszert alkalmazok. Annak érdekében, hogy a kutatási kérdésekre választ kapjak, primer kutatásom során esettanulmányokat fogok készíteni, illetve vizsgálni. Esettanulmány alapú kutatást olyan esetben érdemes alkalmazni, amikor a kutatás alapját képező koncepciók és azok közötti kapcsolat nem vizsgálható izolált módon. Az IT területein gyakran alkalmazott módszer a digitális technológián alapuló pénzügyi szolgáltatások vizsgálatához is alkalmas. FinTech témakörben írt dolgozatomra ezért kiválóan alkalmazható ez a kutatási módszer. A kutatás során kis számú vizsgálati alany szerepel az esettanulmányokban, hogy mélyebb összefüggéseket tudjak feltárni.

Dolgozatomban összesen négy magyarországi FinTech vállalkozáson keresztül szemléltetem, hogy a vizsgált digitális pénzügyi szolgáltatók hogyan alakítják a hazai pénzügyi

megoldások piacát. A vállalkozások kiválasztásánál az egyik fő szempont az volt, hogy eltérő tevékenységi területeken működjenek a FinTech piacon, annak érdekében, hogy több területen okozott változást is be tudjak mutatni. A tevékenységi területek kiválasztásánál a leghangsúlyosabbakat választottam ki a magyar digitális pénzügyi szektorból. Az esettanulmányok elkészítése során többféle adatgyűjtési eszközt alkalmaztam, például internetes források, illetve archívumok, ezen felül az egyik vizsgált cég esetében készítettem egy mélyinterjút is.

Az esettanulmányba bevont vállalkozások darabszámából kifolyólag a kutatási eredmények inkább kvalitatív jellegűek lesznek, nem lehet általánosított következtetéseket megfogalmazni a témában. Az esettanulmányok során azt szemléltetem és értékelem, hogy a szakirodalomban megfogalmazott elméleti koncepciók mennyire valósulnak meg a gyakorlatban. A szakirodalmi források szintetizálása, illetve az esettanulmányokon keresztül megvalósuló vizsgálatok során egyaránt fogok hazai és nemzetközi forrásokra támaszkodni.

3. SZAKIRODALMI ÁTTEKINTÉS

A készpénz létrejöttének elsődleges célja az volt, hogy megkönnyítse az áruk és szolgáltatások cseréjét, ezen a funkciója a pénznek még ma is él. Az 1950-es évektől kezdve egyre gyakrabban jelentek meg új megoldások a pénzügyekben, kezdve a csekkek kibocsátásával, a bankszámlák közötti átutaláson át, a kártyás fizetésen keresztül egészen a manapság már egyre inkább elterjedt mobilfizetésig (Végső, 2020). Ez a trend a 21. században gyorsult fel igazán.

3.1. A PÉNZÜGYI SZEKTOR VÁLTOZÁSAINAK ÁLTALÁNOS BEMUTATÁSA A DIGITALIZÁCIÓ TÜKRÉBEN

A banki ügyfelek egyre inkább az olyan szolgáltatásokat részesítik előnyben, amelyek gyorsak és egyszerű – inkább elektronikus – ügyintézkést kínálnak. Az utóbbi években a banki műveletek egy része már a bankok megkerülésével is végrehajthatóvá vált, így egyre több vállalkozó látta a piaci rést, ahol digitális pénzügyi szolgáltatások nyújtásával viszonylag alacsony tőkebefektetéssel gyors növekedéshez és bevételhez lehet jutni (Kerényi et al., 2018). A fizetési szolgáltatások piacára az utóbbi időben számos új szolgáltató lépett be. Az új pénzügyi szereplők magasabb színvonalú ügyfélélményt kínálva hatalmas befolyást gyakorolnak az inkumbensek (hagyományos pénzügyi szereplők pl. bankok) és ügyfeleik közötti kapcsolatra – átvéve a hagyományos pénzügyi intézmények feladatának (pl. fizetési szolgáltatások) egy részét (EBA, 2018). A globális pandémia csak növelte az új szereplők (kihívók) érdeklődését a pénzügyek területe iránt. A szektort a vírust megelőzően is a digitális trendek formálták, melynek során megjelent az igény az alternatív fizetési modellek iránt. Mindezek hatására megnövekedett aktivitás figyelhető meg a bankokat kihívó szereplők körében, nem csak a B2C (business-to-customer), de a B2B (business-to-business) szektorban is. Korábban a B2B fókuszú pénzügyi szolgáltatók elsődlegesen egyszerű megoldások kínálásával foglalkoztak (pl. számlázás, valutaváltás), viszont egyre inkább törekszenek arra, hogy kiterjesszék a képességeiket és teljeskörű (end-to-end) tranzakciók lebonyolítását tudják támogatni (KPMG, 2021). A pénzügyi szektor új szereplői gyakran nagyösszegű kockázati tőkebefektetést is kapnak a sikeres működésük elősegítése érdekében.

Napjainkban a pénzügyi szolgáltatások nyújtását erőteljesen meghatározza a platformizáció, többek között a PSD2 szabályozással megjelenő open-banki (nyílt bankolás) törekvések és a BigTech vállalatok (pl. Google, Facebook) térnyerése miatt. Az úgynevezett

BigTech-ek olyan technológiai óriáscégek, amelyek széleskörű informatikai szolgáltatásaik mellett az elmúlt időszakban már pénzügyi szolgáltatások nyújtásával is foglalkoznak (Katona, 2021).

A 2019-ben bevezetett PSD2 (Revised Payment Services Directive) egy olyan Európai Uniósi direktíva, amely a bankok számára kötelezővé teszi, hogy az ügyfelek számláihoz – azok beleegyezése esetén – külső, harmadik feles szolgáltatók (Third Party Providers – TPP) hozzáférhessenek pénzügyi és információs szolgáltatásaik végzése érdekében. A PSD2 nyílt bankolási szabályai szerint a felhasználók döntenek el, hogy kinek engedik át pénzügyi adataikat. A bankok feladata pedig az, hogy ezeknek az érzékeny pénzügyi adatoknak az átadása a pénzügyi szolgáltatók számára biztonságos módon történjen. Erre a legmegfelelőbb eszköz a nyílt hozzáférést biztosító alkalmazásprogramozási felület/interfész (API – Application Programming Interface). Az open banking – nyitott bankolás – tehát egy olyan szolgáltatási modell, melyben a banki adathalmaz intelligens, hatékony elemzésével és felhasználásával az új digitális pénzügyi szolgáltatások egyedi igényekhez igazíthatók, ezáltal növelve az ügyfélélményt. A direktíva elsődleges célja a bankpiaci verseny erősítése volt a digitális pénzügyi szolgáltatók bevonásával. Ilyen digitális pénzügyi szolgáltatók lehetnek FinTech (Financial Technology – pénzügyi technológia) cégek, vagy a korábban már említett BigTech cégek, esetleg más szolgáltatók. Az inkumbens szereplők és a digitális pénzügyi szolgáltatók működési feltételeit már a kezdetektől fogva aszimmetria jellemezte. A hagyományos bankokra szigorú szabályok vonatkoznak, míg FinTech cégek elsősorban csak pénzforgalmi szolgáltatásokat nyújtottak diszruptív technológiák felhasználásával, mindezt rendkívül alacsony költségek mellett. Mindeközben a hagyományos bankok viselték a náluk elhelyezett betétek, folyószámlapénzek biztonságos kezelésének költségeit és a betétek után kamatot is fizettek (Müller – Kerényi, 2021). Fontos megjegyezni, hogy FinTech kifejezés alatt érthetjük a digitális pénzügyi szolgáltatókat, a technológia újításokat, illetve magát a digitális pénzügyi szektort is.

A PSD2 szabályai szerint a bankoknak az API hozzáféréseiket a pénzügyi hatóságok nyilvántartásában szereplő számlainformációs (AISP – Account Information Service Provider) és fizetéskezdeményezési szolgáltatók (PISP – Payment Initiation Service Provider) számára ingyenesen hozzáférhetővé kell tenniük. Az úgynevezett harmadik feles szolgáltatók (AISP, PISP) a banki API-kon keresztül csatlakozhatnak rá a bank infrastruktúrájára. Innen – az ügyfelek előzetes engedélyével – tranzakciós adatokat tudnak lekérni, illetve utalásokat tudnak indítani. A PSD2 kötelezte az Európai Bankhatóságot (EBA) arra, hogy készítsen egy központi adatbázist – regiszttert – az EU országokban szolgáltatást nyújtó pénzügyi vállalkozások

bizonyos csoportjairól (pl. elektronikuspénz-kibocsátók, PSD2 szerinti szolgáltatók stb.). Abban az esetben, ha a központi regiszterben nem szerepel az adott pénzügyi szolgáltató, akkor a bank a szolgáltató által kezdeményezett API hívást blokkolhatja. Ennek kiemelt jelentősége van a bankok számára, hiszen visszaélés esetén őket terheli elsődlegesen a felelősség, nem a harmadik feles szolgáltatókat. Mivel a nem megbízhatóan működő API rontja a harmadik feles szolgáltató üzleti lehetőségeit, szolgáltatásának megbízhatóságát és a szolgáltatáshoz kapcsolódó ügyfélélményt is, így a bankoknak erre az esetre tartalékmechanizmust kell kidolgozniuk. Ennek keretében a bankoknak a netbanki interfészeket is használatra kész állapotba kell állítaniuk a harmadik feles szolgáltatók számára. (Németh, 2019a; Németh, 2019b). A számlainformációs szolgáltatók (AISP) a banki API-kon keresztül minél szélesebb körű, tartalmas pénzügyi információ elérhetőségében érdekeltek, melynek érdekében szimbiózisban működhetnek a számlavezetési platformot biztosító bankokkal. (Prágay, 2018).

A digitalizáció hatására megváltoztak a fogyasztói szokások és előtérbe került a magas ügyfélélmény igénye. A pénzügyi piac szereplői körében az új belépők miatt megnőtt a verseny, így annak érdekében, hogy lépést tudjanak tartani a megváltozott igényekkel és meg tudják tartani a piaci pozíciójukat, a legtöbb vállalkozás a technológiát hívta segítségül. A pénzügyek területén elterjedt innovációk révén felgyorsult az adatfeldolgozás és hatékonyabb lett a szolgáltatásnyújtás. A pénzügyi szektorra leginkább hatást gyakorló úttörő technológiai újításokról a következő fejezetben gyűjtöttem össze a legfőbb gondolatokat.

3.2. DISZRUPTÍV TECHNOLÓGIÁK ÉS ÚJSZERŰ ÜZLETI MODELLEK A FINTECH SZÉKTORBAN

A pandémia hatására hazánkban is előtérbe kerültek a digitális megoldások, így az online fizetés lehetősége iránti érdeklődés is növekedett. Ahogy a BigTech-ek és a nem pénzügyi vállalatok egyre inkább nyitnak a beágyazott fizetési, valamint az end-to-end szolgáltatások felé, úgy a B2B fizetési szolgáltatások iránti kereslet is egyre növekszik (MNB, 2021a). A BigTech cégek rengeteg felhasználóval és ebből kifolyólag hatalmas adattömeggel rendelkeznek, aminek segítségével saját platform stratégiát alakítanak ki, a pénzügyi közvetítő rendszer feladatainak növekvő hányadát átveve. A Big Data (nagy adatvagyon) elemzéshez használt eszközök terén is előnyeik vannak (pl. AI-algoritmuskok), aminek segítségével könnyebben meg tudják érteni az ügyfelek igényeit és befolyásolják is tudják őket (Müller – Kerényi, 2021). Az egyre kifinomultabb okoseszközök és azok összekapcsolása elképesztően nagy méretű adathalmazt generálnak. „A Big Data döntési szabályok gyűjteménye és

alkalmazása, vagyis az adatfeldolgozás egy olyan módja, ahol nagymennyiségű, sokrétű és strukturálatlan adatról van szó (Industry4, 2021)”. Ez az adathalmaz azonban – ha megfelelő eszközökkel dolgozzák fel (pl. AI) – akkor hatalmas értékkel bír.

A hagyományos bankokhoz képest a digitális platformcégek és a FinTech (Financial Technology – pénzügyi technológia) vállalkozások sokszor fejlettebbek a Big Data által kínált lehetőségek kiaknázásában. Az általuk üzemeltetett platformokon folyamatosan rögzítik a felhasználók választásait és digitális viselkedését, melyből egy komplett adatbázist hoznak létre. Több éves tapasztalatuknak köszönhetően pontosan tudják, hogy hogyan építsék hatékonyabban az adatbázisaikat, milyen modellek segítségével elemezzék a benne lévő adatokat, és hogyan vezessék vissza a kapott eredményeket az értékesítésbe (Schenk, 2018).

Diszruptív FinTech technológiák közé soroljuk többek között a megosztott főkönyvi technológia, (distributed ledger technology – DLT), alkalmazásprogramozási felület (application programming interface – API), felhő alapú technológia, mesterséges intelligencia (artificial intelligence – AI) és annak egy részterülete: a gépi tanulás (machine learning – ML) technológiákat, melyek alkalmazásával magasabb ügyfélélményt nyújtó szolgáltatásokat tudnak kínálni a digitális pénzügyi szolgáltatók (Müller – Kerényi, 2021). Ezek közül az API-ról az előző fejezetben volt szó a PSD2 szabályozás kapcsán. Ezen újítások egy részének megértésének magasszintű informatikai tudásra lenne szükség, így a technológia IT oldaláról csak érintőlegesen, felszínesen írok a dolgozatomban.

A FinTech technológiákat számos operatív pénzügyi területen tesztelik, hogy minél gyorsabbá és költséghatékonyabbá tudják alakítani a munkafolyamatokat. Az osztott főkönyvi technológia határokon átnyúló történő fizetésre való használata csökkenti a folyamat komplexitását, működési költségeit, gyorsítja az egyeztetési folyamatokat és erősíti a tranzakció transzparenciáját. Mindemellett növeli a KYC (Know Your Customer/Client – ismerd meg az ügyfeled) típusú adatok elérhetőségét, amely az ügyfélazonosítási folyamatokat és azáltal a kockázatkezelést teheti hatékonyabbá. Ugyanakkor, ha a DLT-n alapuló fizetési rendszerek nem tudnak a már meglévő folyamatokkal és infrastruktúrákkal „együttműködni”, akkor az egy átfogó pénzügyi hatékonyságvesztéshez vezethet (FSB, 2019).

A pénzügyek területén is egyre hangsúlyosabbá válnak az olyan hagyományos piactér típusú digitális felületek, ahol a fogyasztók egy helyen érhetnek el különböző pénzügyi és nem pénzügyi termékeket és szolgáltatásokat (Katona, 2021). A FinTech-enabled Marketplace egy hagyományos piactér üzleti modellen alapszik, melynek platformjába közvetlenül bele van építve valamilyen FinTech megoldás (pl. elektronikus fizetés, biztosítás stb.). Ezzel a megoldással a – korábban a vevő és az eladó közé beékelődő – pénzügyi közvetítő (pl. külső

fizetési szolgáltató) kiiktatható a folyamatból, amely által szorosabbá válhat a kereskedő és az ügyfele közötti bizalmi és üzleti kapcsolat (Flint, 2021). A FinTech Marketplace segítségével szélesíthető a célpiac, csökkenthetők az ügyfélszerzési költségek és a rendelés során előforduló fennakadások, sűrűlódások, hiszen a felhasználó egy felületen intéz mindent a teljes vásárlás alatt. Az online piactér és a beépített elektronikus fizetési megoldás kombinációjára kiváló példa az Amazon (piactér) és az azon belül használható fizetési megoldás az Amazon Pay (Adevinta Ventures, 2021).

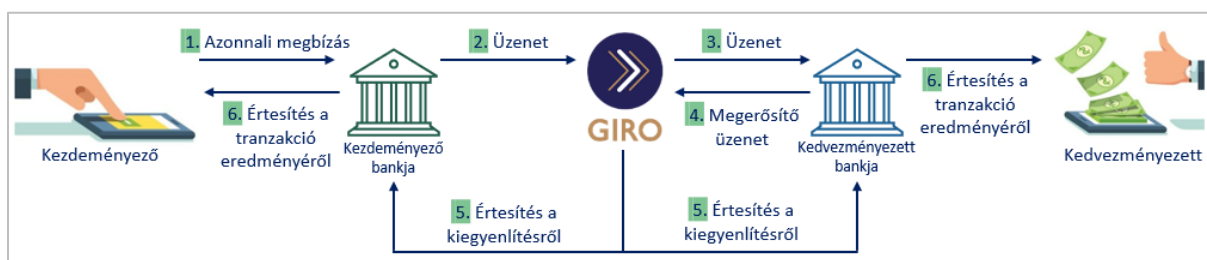
Az infrastruktúra szolgáltatók számítási, tárolási és hálózati erőforrásokat kínálnak az ügyfeleknek. A felhőalapú számítási szolgáltatás árazása jellemzően használatalapú fizetés keretében történik. Ezt a megoldást gyakran IaaS-nek is nevezik, amely az angol „infrastructure-as-a-service” kifejezésből ered. Az IaaS a négy felhőszolgáltatás egyike a szolgáltatott szoftver (SaaS – software-as-a-service), a szolgáltatott platform (PaaS – platform-as-a-service) és a kiszolgáló nélküli megoldások mellett (Azure, 2021). Ennek egy részhalmaza a pénzügyi infrastruktúra szolgáltatók csoportja, akik a már nem feltétlenül felhőalapú infrastruktúrát szolgáltatnak, de mindenképpen valamilyen pénzügyi megoldás technikai hátterét értékesítik (pl. Plaid).

A digitális pénzügyi szolgáltatások nyújtása során tehát számos innovációt lehet segítségül hívni. A hagyományos – készpénz – alapú fizetést is egyre inkább kiszorítják a különböző elektronikus fizetési módok. A bankkártya használat volt az első alternatív fizetési opció, ma azonban már számos lehetőség érhető el mind a kereskedők, mint a vásárlók szemszögéből. Magyarországon az azonnali fizetés bevezetése óta – a vírushelyzet kényszerítő hatását figyelembe véve – egyre népszerűbbek az elektronikus fizetési módok, melyről a következő fejezetben fogok írni.

3.3. MAGYAR HELYZETKÉP AZ ELEKTRONIKUS FIZETÉS VONATKOZÁSÁBAN

A különböző fizetési módok közötti választás mögött egyrészt a szubjektív preferenciák, a megszokás, illetve mélyen gyökerező hiedelmek (pl. a készpénz gyorsasága) állnak. Másrészt sokan a nem kellő mértékű POS terminál lefedettség miatt, kényszerűségből választják a készpénzhasználatot (Végső et al., 2018). A lefedettség országos szintű növelése érdekében már számos kormányi intézkedés született, emellett az azonnali fizetés megjelenésével számos egyéb megoldás is alkalmazható a terminál használatának kikerülésére – mind a kereskedő, mind a vásárló részéről. Az azonnali fizetési rendszert 2019. március 2-án léptették életbe Magyarországon, amely lehetővé teszi, hogy az elküldött pénz (10 milliói

forintos értékhatárig) azonnal (5 másodperc alatt) elérhetővé váljon a kedvezményezett számára az év minden napján, napi 24 órában, belföldi – nem csoportos – forint átutalások esetében. A szolgáltatás jogszabályi előírás alapján minden belföldi banknál elérhető és plusz költség nélkül igénybe vehető. Amennyiben a kedvezményezett a bankjánál regisztrált másodlagos azonosítót, úgy annak ismeretében már akár e-mail címre, vagy mobilszámra is utalhatunk. Ha az utalás körülményei megfelelnek az AFR követelményeinek, akkor a szolgáltatás automatikus. Az azonnali fizetési rendszer működését, folyamatát az alábbi ábra (1. ábra) szemlélteti:



1. ábra: Az AFR folyamatábrája

Forrás: AFR, 2020 (saját szerkesztés)

Ahogy az látszik az ábrán is, nem bonyolódott a fizetés folyamata az AFR bevezetésével, csupán a sebesség az, ami szembetűnő lehet a banki ügyfelek számára.

Magyarországon egy 2019-es felmérés eredményei (Deák et al., 2021) szerint a kiskereskedők pénzforgalma inkább készpénzes, míg a vállalatoknál az átutalások a jellemzőbbek, a nagyobb értékű vásárlásokat inkább bankkártyával rendezik. Rövid távon a készpénzes fizetés költségei alacsonyok, hosszú távon azonban – egy kritikus szintet elérve –, magasabbak a társadalmi költségei, mint az elektronikus fizetéseknek. A készpénzhasználat visszaszorulása az adóelkerülést is csökkentheti. A kártyás elfogadói hálózat fejlettségére vonatkozó kutatások (Kajdi – Nemecskó, 2020) azt mutatják, hogy jelentős eltérések vannak az ország különböző területeit tekintve. A kiskereskedések számára a forgalmukhoz viszonyítva csak jóval drágábban érhető el ez a szolgáltatás, melynek az a fő oka, hogy a bankok a kiskereskedők szegmenséhez kapcsolódó kockázatot kompenzálni szeretnék. A kártyaelfogadás költségei tehát fontos szerepet játszanak a fizetési módok alkalmazása esetében, így az olcsóbb azonnali fizetési megoldások kedvezőbbek lehetnek a kisebb kereskedések, vállalatok esetében. Ezek alapján főként a mikro- és kisvállalkozásokat érdemes célozni közpolitikai intézkedésekkel, annak érdekében, hogy szélesebb körben használtak legyenek az elektronikus fizetési módok. Az azonnali fizetés elterjedése ezen vállalkozások

körében elősegítheti a pénzforgalmi szempontból kevésbé fejlett észak-magyarországi és alföldi régiók, illetve a kisebb községek fejlődését (Deák et al., 2021; Kajdi – Nemecskó, 2020).

A kisebb forgalmú kereskedők számára költséghatékony megoldást kínál a másodlagos számlaazonosító megadásán alapuló fizetési megoldások elérhetővé tétele a vásárlók számára. Ennek az az alapfeltétele, hogy a kereskedő előzetesen regisztráljon egy, vagy több másodlagos számlaazonosítót (mobiltelefonszám, e-mailcím vagy adószám) a bankszámlájához – például internetbanki felületen keresztül – és erről tájékoztassa a vásárlókat. A fizetni kívánó vásárlók a telefonjukra letöltött mobilbanki applikációjukba belépve tudják elindítani az azonnali átutalást a kereskedő által megadott másodlagos számlaazonosítóra. A fizetés sikerességéről, vagyis az áru/szolgáltatás ellenértékének megérkezéséről a kereskedő a saját mobilbanki alkalmazásán keresztül tud tájékozódni. A megoldás nagyobb mértékű közreműködést igényel a vásárló részéről, azonban a kereskedő számára mindenféle többletköltség nélkül bevezethető a törvény által 2021. január 1-je óta kötelezően biztosítandó elektronikus fizetés lehetősége (MNB, 2020). Fontos megjegyezni ugyanakkor, hogy a másodlagos számlaazonosítóra csak átutalást lehet indítani – azaz nem bankkártyás fizetés történik –, mely átutalásnak a költségét a fizető fél viseli. Ez a költség a vásárló bankszámlacsomagjától és a számlavezető banktól is nagyban függ, hiszen, ha a kereskedő eltérő bankban vezet számlát, akkor az utalás bankon kívülinek minősül, ami egyes esetekben szintén magasabb költséget von maga után. A felmerülő költségre a RowanHill Digital (2020) szerint megoldást jelenthet, ha a termékeknek a különböző fizetési módok esetén különböző árat adnak meg a kereskedők. Ez azt jelentené, hogy átutalás esetén a legkedvezőbb az adott termék ára, hiszen ez a kereskedő számára díjmentes. A készpénzes fizetés esetén közepesen drága, ezzel kompenzálva a kereskedő kezelési költségét. Legdrágább pedig bankkártyás fizetés esetén lenne a termék, mivel a kereskedőnek a terminál és a jutalékok miatt ezen fizetési mód esetén jelennek meg a legmagasabb ráfordításai. Bár a megoldás futurisztikusnak tűnhet, de pár éve a QR kódos fizetések és másodlagos számlaazonosítóra történő utalás hazai megjelenése a kiskereskedelemben is távolinak tűnt. Ettől azonban talán realisabb az a megoldás, ha a bankok felülvizsgálják jelenlegi számlacsomagjaikat és olyan termékeket is kínálnak az ügyfeleknek, amelyekkel valóban költségmentes lenne az azonnali átutalással – és az arra épülő a QR kód segítségével – való fizetés is. Ez központosítva is megvalósítható, amennyiben a szabályozó megállapít egy szabványosított hatósági limitet, illetve fontos befolyásoló tényező lehetne a tranzakciós illeték eltörlése is (RowanHill Digital, 2020).

A magyar kereskedők zöme az online tranzakciók lebonyolítása során az úgynevezett háromszereplős fizetési modellt alkalmazza, mert az első kártyaelfogadók erre a modellre

szocializálták a piacot. Ebben a modellben egy adott tranzakcióban a kereskedő (webáruház) és a vásárló közé beékelődik egy kártyaelfogadó szolgáltató, amelynek weboldalán a vásárló megadja a bankkártyaadatait és fizet. A folyamat során a kereskedő a kártyaszámmal és egyéb megadott adatokkal nem kerül kapcsolatba, kizárólag a tranzakció sikerességéről kap visszaigazolást. Mivel a tranzakció végrehajtása közben a vásárlót átirányították egy speciális fizetési felületre, így az ott megadott érzékeny banki adatok biztonságáért a fizetési oldalt üzemeltető kártyaelfogadó felel. A kártyaelfogadó szolgáltató fizetőfelületén általában feltüntethető a kereskedő logója és a céges arculathoz igazodó színvilág is minimálisan testreszabható, de a teljes egyedi arculat általában nem használható. Kétszereplős fizetési modell esetén a vásárló végig a kereskedő felületén marad a vásárlási folyamat lezárultáig, aki a háttérben továbbítja a vásárló által megadott bankkártya adatokat az elfogadó felé. Ebben a modellben a kereskedőt terheli az adatok biztonságának felelőssége. Ahhoz, hogy egy kereskedő a kétszereplős fizetési modellt alkalmazhassa, ahhoz a kártyatársaságok PCI DSS szabványának megfelelő rendszerrel és minősítéssel kell rendelkeznie. Ha a kereskedő rendszere nem felel meg a szabvány által előírt követelményeknek, akkor csak a háromszereplős modellben tud online fizetést lebonyolítani a kereskedő (Schmidt, 2018). A PCI DSS szabványt a 2.5. fejezetben fogom részletesen ismertetni.

Az elektronikus fizetési szolgáltatások közötti átjárhatóság foka nagymértékben hozzájárul azok széleskörű alkalmazásához. A Magyar Nemzeti Bank az azonnali fizetési szolgáltatások közötti átjárhatóság elősegítése érdekében két útmutatót is publikált a 2019-es évben (MNB, 2020). Az első a fizetési folyamatokra vonatkozik, a másik pedig a QR kódokhoz kapcsolódik. Ezek az útmutatók egységes technikai háttérrel adnak a különböző fizetési megoldások létrehozásához. A fizetési folyamatokra vonatkozó útmutató azt mutatja be, hogy adott fizetési helyzetekben hogyan bonyolíthatóak le az azonnali fizetések, illetve a fizetési folyamat egyes lépései alkalmával milyen információáramlás zajlik a résztvevők között. Az útmutatóban szereplő folyamatleírások megkönnyítik, illetve gyorsítják az új fizetési megoldások létrehozását a fejlesztők számára, ezáltal egyszerűbbé válik a piacra lépésük. Másrészt az útmutató alapján kialakított fizetési szolgáltatások esetében egységessé válhatnak a fizetési folyamatok az ügyfelek számára, így a szolgáltató banktól és az alkalmazott mobilfizetési megoldástól függetlenül azonos folyamatban bonyolíthatók le a tranzakciók. A második útmutatóban közzétett QR-kódszabvány az azonnali fizetésre épülő mobilfizetési szolgáltatások közötti átjárhatóságot biztosítja. Egy mobilfizetési megoldás esetében sokféleképpen lehet bevinni a kedvezményezett azonosítására és a fizetés indítására vonatkozó adatokat. A manuális adatbevitel egyszerű és költséghatékony, viszont időigényes. Ezzel

szemben az NFC (Nier Field Communication) vagy Bluetooth-alapú megoldások gyorsak, viszont költséges a fejlesztésük és mélyebb integrációt követelnek meg. Az imént említett két adatbeviteli módszertől sokkal kedvezőbb a QR-kód használata, hiszen alacsony fejlesztési igénnyel létrehozható, és a vásárló részéről is csak minimális közreműködés szükséges a fizetési adatok beolvasásához. Az útmutatóban közzétett szabványosított QR-kód révén az ügyfél a saját mobilfizetési applikációját használva – annak szolgáltatójától függetlenül –, bármelyik szolgáltató által megjelenített fizetési adatokat be tudja olvasni például fizetés kezdeményezés, vagy számla befizetés során (MNB, 2020).

Az elektronikus fizetési megoldások a digitális térben zajlanak, így az adatáramlás során kiberkockázati tényezők is közre játszhatnak. A diszruptív FinTech technológiák és az elektronikus fizetés alkalmazásából, illetve a digitális pénzügyi szolgáltatásnyújtásból eredő kockázatokat a soron következő fejezetben ismertetem.

3.4. A DIGITÁLIS PÉNZÜGYI SZOLGÁLTATÁSOK MIATT FELMERÜLŐ KOCKÁZATOK

A FinTech használata teljesen új kockázatokat is felvethet. Az AI alapú megoldások kockázata abban rejlik, hogy sokszor emberi beavatkozás nélkül mennek végbe a döntési folyamatok, illetve az ügyfelek és a felügyelő hatóságok nem teljesen értik az algoritmusok működését. Az osztott főkönyvi technológia alapú nyilvántartás és ügykezelés elmoshatja a jogi és szabályozási felelősségeket, amelyek eredetileg kétoldalú ügynök-ügynök kapcsolatokra épülnek. Az új technológiák használatából eredő kiberkockázat is megnőtt az adatok vonatkozásában. A személyes adatok védelmére az EU először az Általános Adatvédelmi Rendeletet, vagy másnéven GDPR-t (General Data Protection Regulation) vezette be. Ennek keretében – egyebek mellett – a pénzintézeteknek biztosítaniuk kell az ügyfelek adatainak védelmét. Ezt követően jelent meg a Módosított Pénzforgalmi Irányelv (PSD2), amely szétdarabolta a betéti és fizetési műveletekre, valamint a hitelezésre korábban jellemző egységet, illetve megszüntette a bankok egyik fő feladatát, ami az ügyféladatok védelme alapján a banktitok kizárólagos őrzése (Müller – Kerényi, 2021).

A Módosított Pénzforgalmi Rendelet (PSD2) kötelezővé teszi a bankok számára, hogy az ügyfelek számláihoz – azok beleegyezése esetén – külső, harmadik feles szolgáltatók hozzáférhessenek pénzügyi és információs szolgáltatásaik végzése érdekében. A harmadik feles szolgáltatók (TPP) csak szigorú azonosítási procedúrát követően juthatnak az ügyfelek számlainformációihoz. Azt viszont nehéz ellenőrizni, hogy a TPP alvállalkozói szolgáltatási

szerződést is kötött-e egy másik vállalkozással, mert azáltal kikerülhetnek az adott körből az érzékeny ügyfeladatok. Ilyen szerződést jellemzően digitális alkalmazások, vagy új interfészek kapcsán kötnek a TPP-k. Az utóbbi években a pénzügyi szolgáltatások kapcsán is előtérbe került a digitális alkalmazások használata, a gyorsaság és az elektronikus ügyintézés, illetve a magasabb ügyfélélmény igénye. Az ügyfelek mesterséges intelligencia és azonnaliság iránti nyitottsága azonban csökkentheti, vagy elfedheti a kockázatérzékenységet (Müller – Kerényi, 2021).

A pandémia hatására megnőtt a vállalatok és a fogyasztók digitális jelenléte, ami új támadási felületet biztosított a hackerek számára, akik a korábban bevált rosszindulatú szoftvereket és webes támadásokat még agresszívebben és kifinomultabban használják. Az adathalászat és a személyiséglopás is gyakoribb lett, a mesterséges intelligencia és gépi tanulás fejlődésével pedig a kibertámadások technológiai kifinomultsága is nőtt. A pénzügyi szektor mindig is közkedvelt célpontja volt a kibertámadásoknak, azonban a home-office-ra való átállás (virtuális magán-hálózat a céges műveletekhez) növelte a támadási felületet. Az elektronikus távügyintézés is mindennapossá vált a bankok életében, melynek hatására megjelentek a vírushelyzetre való hivatkozással történő megtévesztések. A központi szabályozás és a kiberbiztonsági szakemberek szoros együttműködése feltétlenül szükséges a kibertámadások elleni stratégiai és szabályozási lépések kialakításában (MNB, 2021a).

Az MNB és a hazai bankszektor közös érdeke, hogy a magyarországi azonnali fizetési szolgáltatás igénybevétele biztonságos legyen, annak széleskörű használatának érdekében. Hazai és nemzetközi felmérések alapján a pénzforgalmi visszaélések kockázatai különböző kategóriákba sorolhatók. Az első ilyen kategória a személyes hitelesítési adatokkal történő visszaélés. Ennek során a csalók a megszerzett hitelesítési adatok segítségével hozzáférnek az ügyfél fizetési számlájához, így átutalások indításával tudnak kárt okozni. A megtévesztésen alapuló visszaélések esetében pedig a csalók valamilyen agyafúrt módon veszik rá az ügyfelet arra, hogy utaljon át pénzt nekik. Például azzal keresik meg a kiszemelt áldozatot, hogy megváltozott a közüzemi szolgáltató számlaszáma, ezért a jövőben máshova – a csaló által megadott számlaszámra – kell utalni a számla összegét. Egy másik bevett csalási gyakorlat szerint egy nem létező indokra hivatkozva csálnak ki az ügyféltől pénzt, miközben banki ügyintézőnek álcázzák magukat. Például olyan ürüggyel, hogy az ügyfél számlájának zárolása miatt a teljes egyenleget át kell utalni egy másik – természetesen a csaló által megadott – számlaszámra, amit a csaló – mint banki ügyintéző – már korábban létrehozott az ügyfél számára (MNB, 2020).

A pénzügyi szolgáltatási folyamatok során az adatok sok szereplőn futhatnak keresztül. A digitális pénzügyi szolgáltatók gyakran alkalmaznak felhőalapú megoldásokat is, azonban ez a fajta hálózatosodás negatív hatást is kiválthat, hiszen így több fajta támadási felület áll az adathalászok rendelkezésére. Hálózatosodás, vagy hiperkonnektivitás alatt azt a jelenséget értjük, amikor egy adott folyamatban részt vevő minden szereplő szoros – információ alapú – kapcsolatban áll egymással. Így amennyiben a hálózati kapcsolati körbe tartozó egyik cég adatai veszélybe kerülnek, úgy az negatív jellegű dominó hatást gyakorolhat a többi hálózatban szereplő cég adataira is. A hálózatban szereplők egymástól való kölcsönös függése az információ áramlás hatékonysága mellett egyben gyengepontként is értelmezhető.

Azokon a piacokon, ahol nagy mértékben koncentrálódnak az adatok, különösen érvényesül a hálózati hatás és csökkennek a pénzügyi közvetítés költségei. Az ilyen piaci szerkezetek csak úgy vonzzák az új belépőket, az így létrejövő koncentrált piaci erő azonban inkább hátrányosnak tekinthető, mint előnyösnek. Erre kiváló példa volt, amikor 2020 novemberében az Amerikai Igazságügyi Minisztérium pereskedett a Visa (fizetési szolgáltató) és a Plaid (FinTech adataggregátor) egyesülése ellen, mely összeolvadás meg is hiúsult 2021 elején. Minden egyes adatmorzsának (pl. fizetéssel kapcsolatos információ vagy az ügyfél által megtekintett termékek listája) van hozzáadott értéke, amennyiben az egy már meglévő hatalmas adathalmazsal kerül összekapcsolásra. Éppen ezért az adatok sokkal értékesebbek a BigTech-ek és a hozzájuk hasonló – sokszínű üzletágakkal és magas színvonalú technológiával rendelkező – cégek számára, amelyek ezáltal digitális monopóliumokká tudnak fejlődni (Feyen et al., 2021).

A platform üzemeltetők a digitális értékesítési csatornákat és az alkalmazásprogramozási felületeket felhasználva zökkenőmentesen be tudják ágyazni a pénzügyi szolgáltatásokat (pl. fizetés, biztosítás) a nem pénzügyi szolgáltatásokba, mint például az e-kereskedelem, vagy közösségi média. Az olyan új infrastruktúrák, mint például a fizetésre és hitelezésre használt API platformok, vagy a kriptovalutákat és stablecoinokat támogató osztott főkönyvi technológiás rendszerek óriási hálózati hatást tudnak generálni. Bizonyos piaci szereplők szerepét képesek átformálni, vagy akár teljes mértékben kiiktatni (Arner et al., 2020).

Látható tehát, hogy számos kockázati faktor került előtérbe az utóbbi években a digitális pénzügyi – és egyéb technológiai – újítások vonatkozásában. Az ügyfeladatok védelme, a pénzügyi piac normális működésének fenntartása és az érzékeny adatokkal dolgozó szolgáltatók megfelelő felügyelete érdekében elengedhetetlen bizonyos szabályozások bevezetése. A kiberkockázati hatások minimálisra szorítása érdekében létrehozott, és a dolgozat szempontjából releváns szabályozói intézkedéseket a következő fejezetben fejtem ki.

3.5. BIZTONSÁGI INTÉZKEDÉSEK ÉS MÓDSZEREK A PÉNZÜGYI KIBERKOCKÁZATOK ELHÁRÍTÁSÁRA

A PSD2 számos kiberbiztonsági előírást tartalmaz, melyek közül az erős ügyfélhitelesítés (SCA – Strong Customer Authentication) emelendő ki, hiszen ez a szabályozás az elektronikus fizetések biztonságosabbá tételét és a felhasználók adatainak védelmét szolgálja. 2019. szeptember 14-től már nem elegendő a bankkártyán szereplő adatokat (név, kártyaszám, CVC-kód) megadni az online fizetések alkalmával. Az elektronikus fizetés terjedésével egyre nagyobb hangsúlyt kell fektetni a vevők adatainak védelmére, melynek egyik eleme a PSD2 által bevezetett többfaktoros erős ügyfélhitelesítés. Az erős ügyfélhitelesítés két különböző – választott – hitelesítési elem használatát írja elő az alábbi három kategóriából: ismeret (jelszó, vagy PIN kód), birtoklás (mobiltelefon, vagy token), illetve biológiai tulajdonság (ujjlenyomat vagy retina mintázat). Az erős ügyfélhitelesítés segítségével az adathalászok visszaélési kísérletei is megelőzhetők, hiszen, ha sikerül is megszerezni az ügyfél jelszavát, az még nem elég egy átutaláshoz, mert még egy hitelesítési elem (pl. ujjlenyomat) szükséges a tranzakció kezdeményezéséhez (MNB, 2020). 2021. január 1-től viszont már nem csak az elektronikusan indított átutalásoknál és a fizikai bankkártyás vásárlásoknál kötelező az erős ügyfélhitelesítés alkalmazása, hanem az online bankkártyás vásárlások esetében is. Ennek értelmében az internetes fizetésnél a bankkártya adatoknak, vagy azoknak és egy SMS-ben kapott megerősítő kódnek a megadása már nem elegendő. Az erős ügyfélhitelesítés mellőzésére azonban vonatkozik egy opcionálisan alkalmazható kivételi szabály, amely a távoli elektronikus fizetési műveletek kezdeményezése esetén ad mentességet, abban az esetben, ha a műveletmegfigyelő mechanizmusok az adott tételt alacsony kockázatúnak ítélték meg. Amennyiben a pénzforgalmi szolgáltató él a kivételi szabály alkalmazásának lehetőségével, vagyis az erős ügyfélhitelesítés mellőzése mellett dönt, akkor az ennek hiányából fakadóan bekövetkezett károkért teljes mértékben az ügyfél számlavezetője felel. Mivel a kivételi szabályok alkalmazásáról a pénzforgalmi szolgáltatók egyedileg dönthetnek, eltérés vehető észre a számlavezetők gyakorlata között. Emiatt az ügyfelek azt tapasztalhatták, hogy nem minden esetben kötelező az erős ügyfélhitelesítés alkalmazása. Az SCA szerint a pénzforgalmi szolgáltatóknak olyan műveletmegfigyelő mechanizmusokkal kell rendelkezniük, amelyek segítségével észlelik a nem engedélyezett vagy csalárd fizetési műveleteket, de a valósidejű alkalmazás nem kötelező. A kockázatokra való tekintettel a banki csalásmegelőzési rendszerek esetében ettől eltérőek MNB elvárásai. A banki rendszereknek képesnek kell lenniük arra, hogy valós időben nagy biztonsággal ismerjék fel azokat a fizetési kísérleteket, amelyek feltehetően nem a pénzügyi

jogos tulajdonosától származnak, vagy nem az ügyfélnél megszokott tranzaktálási sémát követik (MNB, 2021b).

A háromszereplős fizetési modellben egy adott tranzakcióban a kereskedő és a vásárló közé beékelődik egy kártyaelfogadó szolgáltató, amelynek weboldalán a vásárló megadja a bankkártyaadatait és fizet. Kétszereplős fizetési modell esetén a vásárló végig a kereskedő felületén marad a vásárlási folyamat lezárultáig, aki a háttérben továbbítja a vásárló által megadott bankkártya adatokat az elfogadó felé. Ahhoz, hogy egy kereskedő a kétszereplős fizetési modellt alkalmazhassa, ahhoz a kártyatársaságok PCI DSS szabványának megfelelő rendszerrel és minősítéssel kell rendelkeznie. A szabvány céljai és az ahhoz kapcsolható követelmények 6 kategóriába vannak besorolva (1. táblázat), melyek a következők:

1. táblázat: A PCI DSS szabvány céljai és követelményei

Célok	A PCI DSS követelményei
1. Biztonságos hálózat kiépítése és fenntartása	1: Telepítsen és üzemeltessen olyan tűzfal-konfigurációt, amely védi a kártyabirtokosok adatait 2: Soha ne használja a forgalmazó által biztosított alapértelmezett jelszavakat és más biztonsági paramétereket
2. Kártyabirtokosok adatainak védelme	3: Védje a kártyabirtokosok tárolt adatait 4: A kártyabirtokosok adatait a nyitott, nyilvános hálózatokon történő továbbítás esetén mindig titkosítsa
3. Sérülékenység-kezelési program bevezetése	5: Használjon víruskeresőt, és rendszeresen frissítse azt 6: Építsen ki és üzemeltessen megfelelő biztonsági rendszereket és alkalmazásokat
4. Hatékony hozzáférés-ellenőrzési megoldások alkalmazása	7: A kártyabirtokosok adataihoz csak az arra jogosultaknak engedjen hozzáférést 8: A számítógép-hozzáféréssel rendelkező személyek mindegyikéhez rendeljen egyedi azonosítót 9: Korlátozza a kártyabirtokosok adataihoz való fizikai hozzáférést
5. Hálózatok rendszeres figyelése és tesztelése	10: Kövesse nyomon és figyelje a hálózati erőforrásokhoz és a kártyabirtokosok adataihoz való hozzáférést 11: Rendszeresen tesztelje a biztonsági rendszereket és folyamatokat
6. Adatbiztonsági szabályzat bevezetése	12: Vezessen be az adatbiztonságra vonatkozó szabályzatot

Forrás: MasterCard, 2021 (saját szerkesztés)

A PCI DSS (Payment Card Industry Data Security Standard) – azaz a kártyatársaságok adatbiztonsági szabványa – olyan követelmények gyűjteménye, amelyet a Payment Card Industry Security Standards Council dolgozott ki. A szabványt a Visa, a MasterCard, az Amex, a JCB és a Discover hozta létre. Ennek keretében egyértelmű útmutatást adnak a kereskedők számára a kártyaadatok kezeléséhez szükséges biztonsági megoldásokról. Fontos kiemelni, hogy a PCI hatálya alá csak a bankkártya tartozik, a SZÉP kártya és az egészségpénztári kártyák például nem. A szabvány által meghatározott szabályok biztosítják az online tranzakciók biztonságosságát és hogy a bankkártya adatokat ne tudják megszerezni az adathalászok. A követelmények egyértelműek, viszont a megfelelő rendszerek és folyamatok kiépítése, működtetése jelentős mértékű erőforrást igényel. Az aktuális irányelvek nyilvánosan is elérhetők a PCI Security Standards Council honlapján.

A PCI teljes dokumentációja részletes leírást és útmutatót ad arra, hogy a fent felsorolt követelmények részleteiben mit és hogyan várnak el. A dokumentáció értelmezése az ebben tapasztalatlan szakemberek számára kihívást jelentő. A tanúsításhoz szükséges kb. 60 oldalas „self-assessment-questionnaire” (SAQ) angol kérdőív kitöltése, illetve az elvárt minősítés szintje sem mindig triviális kérdés, így a bevezetéshez külső tanácsadók és szakértők bevonása is szükséges lehet. A sikeres minősítést követően rendszeres felülvizsgálat vár a kialakított rendszerre, amit csak megfelelő licensszel rendelkező biztonsági cég végezhet. (Ezen módszerek részletes leírásával nem foglalkozok a dolgozat keretein belül). A bevezetési folyamat összességében milliós összeg is lehet, de az éves fenntartás is több százezer forint körül alakul, ami a kisebb kereskedő cégek számára kivitelezhetetlen, vagy igen megterhelő anyagilag (Schmidt, 2018).

Az eddigi feljegyzések alapján, tekintetbe véve, hogy mennyi fájl kapcsán volt adatvédelmi incidens, vagy másnéven adatsértés, 2020 bizonyult a legrosszabb évnek. Ehhez nagymértékben hozzájárult az, hogy a mobileszközök használata a pénzügyi területeken is kezd elterjedni. Így az eddigiekhez képest még mélyrehatóbb biztonsági intézkedések szükségesek a modernkori veszélyek elhárítása érdekében. A pénzügyi technológiák alkalmazása igényli leginkább az erős kiberbiztonságot, de szerencsére az digitális eszközök a megnövekedett kockázatok mellett is segítenek biztonságos módon megőrizni az érzékeny pénzügyi adatokat. A FinTech biztonságosabbá tétele érdekében az alábbi technológiákat érdemes kiemelni:

- *Többfelhős adattárolás:* A legtöbb pénzügyi intézmény számára nem kielégítő kizárólag egy publikus felhőben való tárolási rendszer szolgáltatásának igénybevétele, ezért biztonsági okokból inkább a privát felhőket részesítik előnyben. Szerencsére a többfelhős adattárolás mindkét preferencia esetére megoldást nyújt. Segítségével átláthatóbbá és biztonságosabbá

válí a vállalkozások adathasználata, miközben az érzékeny adatok számára biztosítva van egy back-up (biztonsági, tartalék) rendszer.

- *Csalás-feltárás mesterséges intelligenciával (AI)*: Az olyan pénzügyi intézmények, mint például a MasterCard a mesterséges intelligencia és a gépi tanulás lehetőségeit kihasználva igyekeznek előre látni- és megelőzni a csalásokat. Ezek a rendszerek adatelemzés segítségével, illetve az ügyfelek digitális viselkedésanalízisével rangsorolják az ügyfeleket kockázati kategóriákba, illetve azonosítják a rendszer gyenge pontjait. A mesterséges intelligencia sokkal hatékonyabban és gyorsabban tud nagymennyiségű adatot elemezni annak érdekében, hogy kiszűrje a jogosulatlan felhasználói tevékenységeket.
- *Secure Access Service Edge (SASE) hálózatok*: A SASE hálózati architektúrák (pl. többfelhős adattárolás) több rendszert egyesít, hogy a biztonsági megoldások a lehető leghatékonyabbak lehessenek. A FinTech területein belül ez nagy kiterjedésű hálózatokat kombinál hálózati biztonsággal, így kínálva egy még átfogóbb felhő alapú szolgáltatást, amely a FinTech cégek védelme mellett nagyobb funkcionalitást is jelent.
- *Blokklánc rendszerek*: A blokkláncok magasbiztonságú decentralizált adatáramlási rendszerek. A speciális technológiának köszönhetően különösen nehezen hack-elhető meg a rendszer, hiszen a láncolatban lévő minden csomópontot egyszerre kellene dekódolni a feltöréshez. A globális pénzügyi piacon ez a technológia gördülékennyé és biztonságossá teszi a tranzakciókat.
- *Szabályozói technológiák (RegTech – Regulatory Technology)*: A folyamatosan változó környezetben a kormányzatok igyekeznek kibővíteni a kiberbiztonsági szabályozásokat. A FinTech biztonságának megteremtésére kiváló eszköz az úgynevezett szabályozói technológia, vagy RegTech alkalmazása. A RegTech a BigData használatával segíti a kormányzati előírásoknak való megfelelést. Az ügyféladatok védelme érdekében ez gyakran magában foglalja az adattitkosítást és olyan módszereket, amelyek lehetetlenné teszik a személyek beazonosítását az adataik alapján (Peters, 2021).

A központi bankok és szabályozó testületek is fel szokták hívni a figyelmet a potenciális kockázatokra, melyek természete a digitalizáció miatt gyorsan változik. A kockázateértékeléshez szükséges adatokat egyre többször mesterséges intelligencia, vagy egyéb technológiai eszközök segítségével gyűjtik össze és értékelik ki. Az információ hatalom, így a szabályozók kiemelt figyelmet fordítanak arra, hogy a FinTech cégek és más pénzügyi szolgáltatók által összegyűjtött digitális ügyféladatokkal ne élhessenek vissza (Kerényi – Müller, 2019).

4. ANYAG ÉS MÓDSZER

A téma újszerűségéből, az iparágban meglévő bizonytalanságokból és annak dinamikus változásából, illetve a rendelkezésre álló hazai és nemzetközi adatok mennyiségének limitáltságából kifolyólag a kutatás eredményessége érdekében zömében kvalitatív módszereket alkalmazok. Annak érdekében, hogy a kutatási kérdésekre választ kapjak, primer kutatásom során esettanulmányokat fogok készíteni, illetve vizsgálni.

Esettanulmány alapú kutatást olyan esetben érdemes alkalmazni, amikor a kutatás alapját képező koncepciók és azok közötti kapcsolat nem vizsgálható izolált módon. Az IT területein gyakran alkalmazott módszer a digitális technológián alapuló pénzügyi szolgáltatások vizsgálatához is alkalmas. FinTech témakörben írt dolgozatomra ezért kiválóan alkalmazható ez a kutatási módszer.

A kutatásaim során kis számú vizsgálati alany szerepel az esettanulmányokban, hogy mélyebb összefüggéseket tudjak feltárni. Az esettanulmányok elkészítése során többféle adatgyűjtési eszközt alkalmaztam, például internetes források, illetve archívumok.

A szakirodalmi forrásokban bemutatásra került trendek, pénzügyi technológiák, kockázatok és szabályozások tükrében esettanulmányokat felhasználva fogom szemléltetni, hogy milyen szolgáltatásai, üzleti modelljei, adatelemzési eszközei és kockázatminimalizáló módszerei vannak a kiválasztott cégeknek. Dolgozatomban összesen négy magyarországi FinTech vállalkozáson keresztül szemléltetem, hogy a vizsgált digitális pénzügyi szolgáltatók hogyan alakítják a hazai pénzügyi megoldások piacát. A vállalkozások kiválasztásánál az egyik fő szempont az volt, hogy eltérő tevékenységi területeken működjenek a FinTech piacon, annak érdekében, hogy több területen okozott változást is be tudjak mutatni. A tevékenységi területek kiválasztásánál a leghangsúlyosabbakat választottam ki a magyar digitális pénzügyi szektorból. Az elektronikus fizetési szolgáltatók közül a Bariont, open banking és adat aggregálás területről a FintechX-et, online fizetések kockázatelemzői közül a SEON-t, összehasonlító platform üzemeltetők közül pedig a Bankmonitort választottam az esettanulmány vizsgálati alanyai közé. Mind a négy választott vállalkozás benne volt a 2016-ban megjelent „25 legígéretesebb magyar háttérű FinTech” listában (T-Systems, 2016), illetve a 2020-ban megjelent „20 legígéretesebb magyar FinTech” listában is (FinTech Group, 2020).

Az esettanulmányok felépítése egyfajta sémán alapszik, melynek első szakaszában az adott vállalat fő profilját és kiemelkedő sikereit emelem ki, majd ezt követően ismertetem a kínált termékeket és szolgáltatásokat részletesebben. Mindeközben arra is kitérek, hogy az egyes vállalkozások milyen biztonsági intézkedések, módszerek és szabályozások mentén végzik a

tevékenységeiket. Ennek során cégenként eltérő módon térek ki az esetleges kötelező és „extra” biztonsági módszerekre, szabályozásokra. Végül minden vállalkozás esetén röviden összefoglalom, hogy az adott cég milyen diszruptív technológiát alkalmaz, illetve, hogy véleményem szerint miben rejlik a kockázata.

A publikusan elérhető forrásokon túl, a Barion esettanulmányába beillesztettem a Barion alapítójával, vezérigazgatójával készített mélyinterjú anyagait, ezáltal naprakész, primer forrásból kapott információval tudtam kiegészíteni az esettanulmányt. A mélyinterjú online formában került lebonyolításra a Cisco Webex alkalmazás használatával, melynek során négy szemközt beszélgettünk az interjú alanyával. Az interjú hanganyagát – előzetes engedély mellett – okostelefonnal rögzítettem. A nem várt kérdések elkerülése végett az előre megfogalmazott kérdéssort e-mail formájában továbbítottam a Barion vezérigazgatójának. A kérdéssor kialakítása során meghatároztam egy fő irányvonalat, amely mellett a kapott válaszok alapján spontán kérdések is felmerültek, ezek együttesen elősegítették a témába való mélyebb betekintést. Az alapkérdések zömében nyitott kérdések voltak, így az interjú alanya bővebben ki tudta fejteni a gondolatait, illetve kialakulhatott egyfajta beszélgetés is. A spontán kérdések főleg pontosító kérdések voltak, vagyis a kapott válasz elhangzása után kértem az interjú alanyától további részleteket, esetleg példákat.

A SEON Technologies Kft. kockázat elemző és csalás megelőző rendszerrel foglalkozik. Ebből kifolyólag a biztonsági szabályok bemutatását nem részleteztem, hiszen a vállalkozás minden tevékenysége valamilyen formában biztonsági intézkedésnek tekinthető.

Az esettanulmányokkal azt fogom szemléltetni, hogy a szakirodalomban megfogalmazott elméleti koncepciók mennyire valósulnak meg a gyakorlatban. Az esettanulmányba bevont vállalkozások darabszámából kifolyólag azonban a kutatási eredmények inkább kvalitatív jellegűek, nem lehet általánosított következtetéseket megfogalmazni a témában.

5. EREDMÉNYEK ÉS AZOK ÉRTÉKELÉSE

Az elmúlt években a FinTech vállalkozások B2C (business to customer) és B2B (business to business) üzleti modellben egyaránt nyújtottak szolgáltatásokat hazánkban. Előbbi kategóriában Magyarországon a legismertebb szolgáltatók a Simple, a Koin, a Bankmonitor, a Revolut, a TransferWise vagy a PayPal társaságok. Az utóbbi kategória meghatározó területe a hagyományos pénzügyi szolgáltatók működését – például a hitelminősítést, a csalás megelőzését – támogató megoldások. A legismertebb megoldások például a Blueopes, az Aggreg8 (FintechX), vagy a SEON. 2020-ban megalapították a MAFISZ-t (Magyar FinTech Szövetség), melynek célja, hogy elősegítse a magyarországi FinTech piac résztvevőinek (startupok és érett vállalkozások, inkubátorok és akceleratorok) együttműködésének, érdekképviselésének és érdekérvényesítő képességének erősítését, valamint a szektor versenyképességének növelését. Az alapító tagok között szerepel a Barion és a Bankmonitor is (MAFISZ, 2021).

Dolgozatomban esettanulmányokat felhasználva összesen négy magyarországi FinTech vállalkozáson keresztül szemléltetem, hogy a vizsgált digitális pénzügyi szolgáltatók hogyan alakítják a hazai pénzügyi megoldások piacát. A vállalkozások kiválasztásánál az egyik fő szempont az volt, hogy eltérő tevékenységi területeken működjenek a FinTech piacon, annak érdekében, hogy több területen okozott változást is be tudjak mutatni.

Az elektronikus fizetési szolgáltatók közül a Bariont, open banking és adat aggregálás területről a FintechX-et, online fizetések kockázatelemzői közül a SEON-t, összehasonlító platform üzemeltetők közül pedig a Bankmonitort választottam az esettanulmány vizsgálati alanyai közé. Mind a négy választott cég benne volt a 2016-ban megjelent „25 legígéretesebb magyar háttérű FinTech” listában (T-Systems, 2016), illetve a 2020-ban megjelent „20 legígéretesebb magyar FinTech” listában is (FinTech Group, 2020).

A bemutatott vállalkozások esettanulmányainál először egy általánosabb cégbemutatót tüntetek fel, melynek számadataihoz többek között az OPTEN (2021) honlapját használtam fel. Ezt követően a cég fő profilját és kiemelkedő sikereit mutatom be, majd a kínált termékek/szolgáltatások részletesebb bemutatása következik. Végül ismertetem, hogy az egyes vállalkozások milyen biztonsági intézkedések mellett végzik a felsorolt tevékenységeiket. (A SEON Technologies Kft. kockázat elemző és csalás megelőző rendszerrel foglalkozik. Ezen cég esetében a biztonsági szabályok bemutatását elhagytam, hiszen a vállalkozás minden tevékenysége valamilyen formában biztonsági intézkedésnek tekinthető.)

5.1. A BARION PAYMENT ZRT. ESETTANULMÁNYA

A Barion Payment Zrt. (2. táblázat) lakossági és vállalati üzletágban is foglalkozik elektronikus pénzforgalmi ügyletekkel, amely eddig alapvetően kereskedelmi banki tevékenység volt. A Barion az első olyan magyar vállalkozás, amely elektronikus pénzkibocsátási (e-money) licenccel rendelkezik, amelyre alapozva egyszerűsített ügyfél-azonosítási (KYC – know your customer) folyamat mellett gyorsabban akvirálhat lakossági és üzleti ügyfeleket. Vállalati üzletágban webshopok számára kártyás fizetési megoldást szolgáltat (B2B), lakosság számára pedig P2P (peer-to-peer) pénzküldési lehetőséget (pl.: mobilfizetés) nyújt (T-Systems, 2016; FinTech Group, 2020).

2. táblázat: A Barion Payment Zrt. alapvető adatai

Barion Payment Zrt.			
Alapítás dátuma:	2015.06.30.	Nettó árbevétele:	713 858 eFt
Fő profilja:	Elektronikus fizetések lebonyolítása		

Forrás: OPTEN, 2021 (saját szerkesztés)

2017 decemberében a Barion 2 millió eurós befektetést kapott a cseh alapítású Home Credit-től (a PPF Group tagja), majd újabb befektetést kapott 2020 áprilisában a londoni székhelyű Financial Services Capital-tól (Barion Payment Zrt., 2021). Kiss (2021a) elmondása szerint ahhoz, hogy a Barion nagyobb tudjon előre lépni további kockázati tőkebefektetési kör szükséges. Számos egyéb terület mellett fontos lenne az eddigiek fejlesztése, így a befektetésre vonatkozó tárgyalások már meg is kezdődtek, folyamatban vannak. Annak érdekében, hogy a Barion nemzetközi szinten is függetleníteni tudja magát – vagyis, hogy fizetési szolgáltató, közvetítői szerepéből kilépjen – idővel el kell érnie azt, hogy bizonyos piacokon (vagy akár az összes piacon) közvetlenül a kártyatársaságokhoz tudjon csatlakozni. Ennek a fejlesztési költsége, a licenc díjai, illetve az éves díjai rendkívül jelentősek.

A legfontosabb sikertényezők közül – amelyek hozzájárultak a Barion sikeréhez – az első az időzítés, vagyis a jó ötlet megvalósításához jókor kellett lenni jó helyen, amihez szerencse kell. Másik fontos tényező a csapat, a Barionnál dolgozó embereknek nincsen meg az a nagyvállalati, banki, pénzügyi piaci tapasztalata. Képzett szakemberekről van szó, akik nincsenek befolyásolva a kialakult status quo-val, emiatt nem a hagyományos, bevett folyamatokban, illetve módszerekben gondolkodnak. Egy hagyományos banki, vagy pénzügyi

szektorból érkező dolgozó a konzervatív gondolkodást képviseli, ami nem illeszthető össze a Barionra jellemző FinTech gondolkodásmóddal. Fontos a dolgozói összetétel szempontjából, hogy a Barionnál sok az olyan munkavállaló, aki pl. SQL-ben képes programozni. Ez a vezetőségre is igaz (pl. CFO), ami általában nem nagyon jellemző egy banki vezetőre. Ebből kifolyólag a Barion vezetősége is hatékonyabb, mint egy banki vezető általában. Szintén fontos sikertényező a kitartás, vagyis a felmerülő akadályok megoldására ki kell találni valamilyen alternatív megközelítést – legyen szó akár egy tárgyalásról az MNB-vel, vagy a Pénzügyminisztériummal, hogy szükséges lenne egy adott törvény, vagy rendelet módosítása (Kiss, 2021a). Fontos megjegyezni, hogy az élvonalban járó FinTech vállalkozások mindegyike diszruptív technológiákkal dolgozik. Ezen technológiák alapjainak megértése a dolgozók, illetve a vezetőség részéről segít elkerülni az AI alkalmazásából eredő, döntéshozatalhoz kapcsolódó kontroll hatékonyságvesztését.

A Barion jelenleg 5 országban nyújtja Smart Gateway megoldását, amely egy teljesen hazai fejlesztésű, bankoktól független fizetési kapu. Az ehhez szükséges szerződést online meg lehet kötni néhány percen belül, integrálása is rendkívül gyorsan elvégezhető a legtöbb nagyobb e-kereskedelmi platformhoz elérhető különféle plug-inoknak és library-knak (könyvtáraknak) köszönhetően. Használatával a vásárlók bármilyen készülékről gördülékenyen fizethetnek, kijelző mérettől, operációs rendszertől és böngészőtől függetlenül (Barion Payment Zrt., 2021) – ami nem mondható el minden elektronikus fizetési szolgáltatóról, pl. az ApplePayról sem. Véleményem szerint a Barionnak ez a fajta megközelítése nagyobb piacok megszerzését teszi lehetővé számukra.

A Barionban a Smart Payment Gateway esetében nincsen csatlakozási díj, illetve havidíj sem, emiatt a kis- és közepes vállalkozások tömegei kezdték el használni. A szolgáltatás feltételei lehetővé tették, hogy a kevés tranzakcióval rendelkezők is tudjanak online fizetés esetén kártyát elfogadni. Ma már több, mint 11.600-700 kereskedő, illetve adószámos magánszemély veszi igénybe a Payment Gateway-t. Azért lehetnek ingyenesek a fent említett tételek, mert a Barion automatizálta a belépési folyamatokat (on-boarding). Ezáltal egy olyan folyamat jött létre, amely a lehető legegyszerűbb, teljesen papírmentes, a lehető legkevesebb idővel, vesződséggel és költséggel jár mind a két fél számára (Kiss, 2021a). Meglátásom szerint a magas ügyfélélmény – melynek meghatározó része az automatizált ügyintézés és az alacsony díjszabás – az egyik legfontosabb fogyasztói döntési kritérium a digitális pénzügyi szolgáltatások igénybevételével, illetve digitális pénzügyi szolgáltató megválasztásával kapcsolatosan.

A Barion honlapján a riportok, az adatexport lehetőség, valamint rendszeresen kiküldött számlalevél segítik az üzleti folyamatokat, illetve a hivatalos elszámolást. Mivel a bankkártya-

számokat egy rendszer tárolja, így azok használatához elegendő a regisztrált e-mail cím és jelszó megadása. A Barion csökkenti a kereskedő bankkártya visszaélésekből származó kockázatát, hiszen verifikált kártya esetén biztosítja a visszaélés elleni védelmet (Barion Payment Zrt., 2021).

A Barion Parkolás és Barion Autópálya-matrica használatának előfeltétele a Barion alkalmazás telepítése. A parkolási díj és az autópálya-matrica kiegyenlítése az ügyfél Barion számláján nyilvántartott e-pénz egyenleg terhére történik, melynek feltöltéséről a felhasználó köteles gondoskodni. Mindkét lehetőség esetében a szokásos, jogszabályban meghatározott díjat fizeti a felhasználó, a Barion semmilyen extra költséggel nem terheli az ügyfelet a szolgáltatás igénybevételekor. A Barion honlapján közzétett ÁSZF szerint vannak azonban kényelmi díjak: parkolás esetében ez 50Ft, autópálya-matrica esetében pedig jármű típustól, illetve hatókörtől és időszaktól függően 100-2.500Ft körül alakul (Barion Payment Zrt., 2021). A Nemzeti Mobilfizetési Zrt. az általa kényelmi díjnak nevezett tételeket gyakorlatilag kiszámlázza a Barion felé, aki minimális hasznot tesz az alap összegre. Így az elnevezés és a kényelmi díjak összegének nagyrésze központi (Kiss, 2021a).

A Barion Market a Barion Alkalmazáson keresztül elérhető olyan online piactér/szolgáltatás, melynek célja, hogy a kereskedők (árut vagy szolgáltatást értékesíteni kívánó eladók) és a felhasználók (árut vagy szolgáltatást vásárolni kívánó vevők) egymásra találását és kereskedelmét piactérként elősegítse. A Barion Market szolgáltatását kizárólag az aktivált Barion tárcával rendelkezők vehetik igénybe, az igénybevétel teljesen díjmentes. A Barion Marketen „boltot nyitó” kereskedőnek azonban market díjat köteles fizetni, melynek mértéke egyedi megállapodásban kerül rögzítésre. Természetesen ezen díjak kiegyenlítése a kereskedő Barion tárcájának megterhelésével történik azok esedékességekor. A vásárlások ellenértékének kiegyenlítése a Barion Smart Gateway-en keresztül Barion tárcával történik. A kereskedő a Barion Market Díj keretében jutalékot is fizet a Barion számára a sikeres Barion Smart Gateway-en keresztül történt vásárlások összege alapján. Sikeres vásárlás alatt azt érti a Barion, hogy a vevő kifizette az árut/szolgáltatást – függetlenül attól, hogy a jövőben a vásárlás alapját képző jogügylet meghiúsul-e vagy sem (pl. a vevő visszaküldi a terméket). A Market díj nem foglalja magában a Smart Gateway-en keresztül történő fizetések igénybevétele kapcsán felmerülő díjakat. Látható tehát, hogy a felhasználók számára teljesen ingyenes megoldás tele van „rejtett” és egyedileg meghatározott költségekkel a kereskedők számára (Barion Payment Zrt., 2021). A Barion Market megoldás általános megnevezése a FinTech-enabled Marketplace, melyben a Barion a tradicionális piacteret (marketplace) kiegészítette egy FinTech szolgáltatással: a fizetéssel (payment), így a Barion Market felhasználói mindent egy

helyen, kényelmesen és gyorsan tudnak intézni. Ezen szempontok egyre meghatározóbbá válnak a fogyasztói preferenciák esetében, tekintve a jelenlegi FinTech trendeket.

Barion tárcából bármely bankszámlára történő utalás tranzakciós illeték mentes, azaz a bankok által felszámított 0,3%-os tranzakciós illeték + utalási díjjal szemben a Barion tárcából indított utalások esetén 0,1% (min. 50Ft) a teljes költség, így további megtakarítások érhetőek el. A regisztráció és a Barion mobil alkalmazás, valamint a pénz fogadás/küldés szintén ingyenes, nincs belépési vagy havi díj. Az egyenleg feltöltésének és visszaváltásának vannak díjai, de a banki átutalással történő feltöltés ingyenes (Barion Payment Zrt., 2021). Látható tehát, hogy a Barion rendkívül alacsony költségeivel igyekszik minél több ügyfelet szerezni. A Barion a fent említett tételeken felül minden egyes díjat feltüntet a honlapján (Jelenlegi díjak & Feltételek), amelyek nem egyedi megállapodáson alapszanak, így egy átláthatóbb díjszabást tesz nyilvánossá a jövőbeli ügyfelek és felhasználók számára.

A Barion Pixel egy java script alapú mérőkód, amely a kereskedő weboldalán kerül elhelyezésre és a weboldal látogatóinak aktivitását követi, a weboldal látogatók böngészőjében elhelyezett cookie-k (sütik) segítségével. A Barion Pixel a weboldalt látogatókról, és azok böngészési szokásairól gyűjt adatokat, mely adatokat a Barion csalásmegelőzési célból kockázatelemzésre és – értékelésre (alap csomag), valamint marketing célból hirdetések, ajánlások személyre szabása érdekében viselkedési szokások vizsgálatára (teljes verzió) használja. Ez utóbbi sütik használata kizárólag a weboldalra látogató hozzájárulása esetén lehetséges. A szolgáltatását igénybe vevő kereskedő köteles saját költségére implementálni a Barion Pixelt, a sütik működése közben a kereskedő semmilyen személyes adatot nem kap meg (Barion Payment Zrt., 2021). A sütik működése által egy gépi tanuláson (AI részhalmaz) alapuló rendszer látja, hogy az adott felhasználónak milyen eseményei vannak, vagy éppen mit csinált. Az esemény, illetve annak paramétereinek a figyelembevételével a rendszer a különböző felhasználókat különböző szegmentumokba sorolja (Kiss, 2021a). Véleményem szerint az ilyen mélységű adatgyűjtés ugyan nem ritka a BigData lehetőségeit kihasználók körében, ugyanakkor kiemelt kockázati faktort jelenthet. Az érzékeny pénzügyi-, és ügyféladatokat kiszivárgása az ügyfelek GDPR jogainak megsértése mellett visszaélésre ad lehetőséget a csalók számára. Az adathalászok az egyre kifinomultabb módszereinek köszönhetően még a magas biztonságú rendszerekbe is képesek betörni, így a kiberbiztonsági intézkedések folyamatos fejlesztése elengedhetetlen.

A Barion a kereskedők számára olyan üzleti modellt alakított ki, amelynek része a Big Data adatvagyonában rejlő lehetőségek hasznosítása. Ezáltal kevésbé látható módon jut bevételhez: lehetőséget ad a kereskedőnek, hogy célzott ajánlatokat juttassanak el a vevőkhöz,

azok vásárlási szokásainak alapján. Kiss (2021a) szerint a Barion egy FinTech és egy AdTech (advertising technology – hirdetés technológia) cég keveréke. A fizetési szolgáltatások szektorában vagy költségmegtakarítással, vagy hatékonyabb működéssel lehet versenyelőnyre szert tenni. A Barion – mint FinTech cég – hatékonyabban, alacsonyabb költségek mellett tud fizetési szolgáltatást nyújtani egy nagyobb bankhoz, vagy egyéb pénzügyi szervezethez képest. Abban az esetben viszont, ha ezek az inkumbens szereplők is elkezdnek költséget optimalizálni, akkor egy költségoptimalizációs verseny alakul ki a két tábor között. Ez nem tekinthető jó piacnak, hiszen ilyen körülmények között nem – vagy csak nehezen – lehetne profitot termelni. Ezt realizálva, a Barion a költséghatékony fizetési szolgáltatása mellett másik fronton is differenciálja magát az inkumbensektől. A fizetési kapu szolgáltatás igénybevételekor a kereskedő dönthet arról, hogy alacsonyabb díjszabás ellenében adatot szolgáltat a Barionnak az ügyfeleiről – azok előzetes beleegyezése mellett. Az így begyűjtött adatok monetizációjára nagy hangsúlyt fektet a Barion, hiszen ezáltal egyrészt tudja a kereskedőt segíteni abban, hogy még több vevőre tegyen szert, másrészt jelentős bevételi forrást jelent ez a vállalkozásnak, azaz win-win szituációról van szó. A Barion tehát egy új vevőmegtartó és vevőszerző marketing eszköz is részben, amely használata díjhoz kötött, de nem kötelező. Nagyságrendileg kb. 2000 kereskedő él az adatmegosztásban rejlő lehetőséggel jelenleg, és olyan nagy brand-ek hirdetnek Barion adatokkal, mint például az IKEA, a Heineken, a Bosch, a Honda vagy a Philips. Kiss (2021a) szerint sokféle területről van bevétele a Barionnak. A két legjelentősebb azonban a Barion Smart Gateway tranzakciós díja, illetve az adatmonetizációs bevételek. Ezen kívül megemlíthető még a Barionos parkolás, vagy autópálya matrica bevétele is.

A Barion már több országban is jelen van Európában, ebből a szempontból – fizetési szolgáltatói oldalról – versenytársnak a nagyobb nemzetközi szereplők tekinthetők, úgy, mint a Stripe, a Mollie, Checkout.com. Csehországban leginkább a GoPay, vagy a ComGate, lokális piacot (Magyarország) tekintve pedig a CIB és az OTP Simple a legjelentősebb versenytárs. Az adatmonetizációt tekintve alapvetően a hirdetők dönthetnek, hogy kinek az adatait használják a kampányaikban (pl. programmatic hirdetések esetén), így ilyen téren a Google, illetve a Facebook is versenytársnak tekinthető. Attól azonban nem fél a Barion, hogy valamelyik versenytárs kiszorítaná a vállalkozást egy adott piacról (Kiss, 2021a). A FinTech szektor fejlődésének egyik alapkőve a versenytársak jelenléte, illetve nyomása, hiszen a piaci verseny hatékonyságjavuláshoz vezet. A piaci pozíció szoros összefüggésben van az ügyfélélménnyel, aminek része az árazás, így a magas versenynek köszönhetően a fogyasztók valószínűleg

olcsóbban tudnak adott szolgáltatásokat igénybe venni egy oligopol vagy monopol piacon elérhető szolgáltatásokhoz képest.

A Barion erősíteni akarja a nemzetközi terjeszkedését. Jelenleg a boltjaik kb. 10%-a külföldi, 90%-a magyar, de ezt az arányt hosszú távon meg szeretnék fordítani. Ennek egyik fő oka a hazai szabályozásra vezethető vissza, hiszen a szabályoknak való megfelelés egyben versenyhátrányba is hozza a vállalkozást nemzetközi szinten. A három legfontosabb szabályozási tényező ezek közül az az írásbeliség, az „on-boarding”-nál az adatkör, illetve a tranzakciós illeték és a kapcsolódó limitek. Az írásbeliség fogalma meglehetősen speciális a magyar szabályozásban, melyre kiváló példa az online bankszámla-, vagy hitelszerződés kötése, amely esetében a magyar joggyakorlat szerint minősített digitális aláírás szükséges az ügyfél részéről. Ez nemzetközi szinten nincs így, a Revolut-os számla esetében például a regisztráció elég az „on-boarding” folyamat során. A másik ilyen terület az szintén az „on-boarding”-hoz kötődik, azon belül is az az adatkör, amit be kell gyűjtenie a Barionnak. A magyar szabályozás rendkívül sok adatot kér, aminek jelentős részét nem tudja leellenőrizni a vállalkozás (pl. anyja neve). Az ügyfél számára panaszra ad lehetőséget, hogy miért kér be olyan „extra” adatokat a vállalkozás, amelyet nem tud leellenőrizni. Számos ország rendszerében nincs benne például a tényleges tulajdonosnak (UBO – ultimate beneficial owner) a születési helye, amelynek bekérése megint furcsa lehet az ügyfelek szemszögéből. Az utóbbi időben a szabályozás ezen része enyhült, hiszen a magyar adatkörben szereplő adatokat továbbra is be kell kérni, de azokat az adatokat, amiket nem lehet leellenőrizni, azt csak bekérni szükséges – ellenőrizni nem. Az „indokolatlan” adatbekérést nem értik az ügyfelek, és további kellemetlenséget okoz az, hogy az adatbekérés miatt hosszabbá válik a folyamat. Emellett a Barion nem kooperálhat olyan olcsó és gyors „on-boarding”-ot garantáló nemzetközi szereplőkkel, akik nem kezelik a magyar adatkör szerinti kötelező adatokat. Ezeken felül említésre méltó még az, hogy a különböző limitek forintban vannak megadva, nincs euróban kifejezett limit. Ebből kifolyólag a Barionnak a külföldi szolgáltatásnyújtása során át kell konvertálnia a limitek összegét – a forintnak megfelelően –, ami miatt folyamatosan változnak a limitek a külföldi ügyfelek számára (Kiss, 2021a). A szabályozás visszafogó hatását véleményem szerint minden FinTech vállalkozás érzékelheti – hazai és nemzetközi viszonylatban is –, hiszen a diszruptív technológiák és az innovatív ötletek alapvetően mindig megelőzik a szabályozást. Pontosabban, ha eddig nem látott megoldás lát napvilágot, akkor arra vagy nem lesz megfelelő szabályozás, ami sérti a tiszta versenyt, vagy a korábbi szabályozást kényszerítik rá az innovációra, ami negatívan hat a további fejlesztésekre.

A PSD2 alapján 2019. szeptember 14-étől kötelező alkalmazni a fizetési szolgáltatóknak az úgynevezett erős ügyfélhitelesítés (SCA: Strong Customer Authentication) módszerét. A Barion 2020. november 30-án kapcsolta be az erős ügyfélhitelesítést (3DS2) a fizetéseknél – Magyarországon elsőként. Ha a Barion a fizetés során megadott adatok elemzése kapcsán úgy gondolja, hogy kell extra megerősítést kérni (pl. SMS), akkor a Barion felületén belül fog erre vonatkozó utasítás megjelenni és ezt a Barion kezeli (Barion Payment Zrt., 2021). Meglátásom szerint ez a fajta szubjektív megítélés nem garantálhat teljeskörű biztonságot fizetés során.

A Barion rendelkezik a bankkártya társaságok által megkövetelt PCI DSS tanúsítvánnyal, így jogosult bankkártya adatokat kezelni, mely az ügyfél számára ingyenes. A Barion tanúsításához szükséges biztonsági vizsgálatot (network scan) az amerikai Comodo HackerGuardian folytatta le, hiszen a folyamatot csak megfelelő licensszel rendelkező biztonsági cég végezheti. A sikeres minősítés után a kialakított rendszer ellenőrzését negyedévente újra el kell végezni. A bevezetési folyamat milliós összegbe kerül, fenntartás költsége pedig több százezer forinttól kezdődik. A PCI DSS szabvány betartása igazodik az e-pénz kibocsátói engedély megszerzéséhez kötelezően előírt COBIT alapú információbiztonsági elvárásokhoz, amely alapján a cég működik. Ezen felül egy olyan biztonsági rendszert fejlesztett a Barion, amely nemcsak az internetes kalózkodtól (hackerektől), hanem a cég saját munkatársaitól is megvédi az adatokat. Így például a vállalat egyetlen munkatársa sem tud egyedül hozzáférni ahhoz a titkos kulcshoz, amivel a kártya adatokat vissza lehet fejteni (Barion Payment Zrt., 2021).

A Barion szerverek biztonságát az MNB előírásai szerint alakították ki, a fizetéshez szükséges bankkártya adatok és jelszó megadása előtt azonban feltétlenül szükséges ellenőrizni, hogy a Barion biztonságos szerverén vagyunk-e. Ezt onnan tudhatjuk biztosan, hogy a böngésző zöld színnel és egy lezárt lakat ikonnal jelzi, ha a weboldal/fizetés biztonságos, és a fizetőoldal tulajdonosát Barion Payment Inc [HU] néven azonosítja.

Az előbbi bekezdésekből egyértelműen kiderül, hogy a Barion kiemelt fontossággal kezeli az ügyfelek, illetve a felhasználók az adatainak védelmét. A Barion további megállapodást kötött a SEON Technologies Kft.-vel, amely az online bankkártyás fizetések és autentikációs pontok kockázatelemzésével foglalkozik. Kiss (2021b) szerint a Barion Smart Gateway fizetési rendszerébe beépített SEON eszköz a bankkártyás visszaélési próbálkozások több, mint 80%-át ki tudja kiszűrni. Egy algoritmus a csalás kockázatának esélye szerint osztályozza a vásárlásokat, így, ha nagy a csalás valószínűsége, akkor a rendszer automatikusan blokkolja a tranzakciót. A SEON cég bemutatása és a Barionnal való kapcsolata a SEON esettanulmányában részletesebben kifejtésre kerül.

A PCI a legmagasabb szintű elvárás a Barion felé, melynek kötelező eleget tenni. A SEON eszközének beépítésével minden online tranzakcióra kockázatelemzés történik. Abban az esetben, ha a kockázat analízis eredménye azt mutatja, hogy alacsony kockázati besorolású a fizetés, illetve a kereskedő azt szeretné, hogy az ügyfeleinek minél gördülékenyebb legyen a fizetése, akkor kérheti azt a kereskedő, hogy ne legyen erős ügyfélhitelesítés az adott fizetésre. A kártya kibocsátó dönthet úgy, hogy nem fogadja el a kereskedő kérését és mégis elvégzi az erős ügyfélhitelesítést, de úgy is dönthet, hogy elfogadja a kereskedő kérését. Abban az esetben, ha a SEON kockázatelemzése azt mutatja, hogy a tranzakciónál olyan paraméterek, tények merülnek föl, ami alapján egy csalásról lehet szó, akkor a Barion visszautasítja a kereskedő kérését arra vonatkozóan, hogy az adott tranzakció egy erős ügyfélhitelesítés nélküli fizetés legyen. Ha mégis sikerrel járnak a csalók és ezt a kártya tulajdonosa jelzi, akkor tud pénz visszatérítést kérni. Volt is egy komolyabb precedens a Barion életében, melynek során tízmilliós nagyságrendű csalással kísérleteztek az elkövetők, melynek nagyrészt megfogta a rendszer. A kártyaadatokkal való visszaélések azonban a 2021. január elsejétől bevezetett erős ügyfélhitelesítés miatt nagyon visszaestek, elenyésző lett a számuk a korábbiakhoz képest (Kiss, 2021a). Ebből is látszik tehát, hogy a Barion a kötelező érvényű szabályokat vezette be, melyek viszonylag magas csalásmegelőzési rátát biztosítanak, teljeskörű védelmet azonban így sem tud garantálni a vállalkozás.

A SalesForm (2021) egyik cikkében összegyűjtötte a szubjektív pro és contra érveket (3. táblázat) a Barionos fizetés bevezetésével kapcsolatosan egy kereskedő szemszögéből, melyet kiegészítettem a saját szubjektív véleményemmel:

3. táblázat: A Barionos fizetés bevezetése mellett- és ellen szóló érvek

PRO	CONTRA
• Olcsó: Ha nincs más bankkal kártya elfogadó szerződésünk, akkor 100mFt-ig 0% a tranzakciós díj, azt meghaladóan pedig 0,5% – 1% között mozog (a bankok 1,6%-ot kérnek). Nincs csatlakozási díj sem. Az OTP jelenleg 49.000 Ft + áfa egyszeri csatlakozási díjat kér. • Nem kell bankszámlát nyitnunk, mert a meglévő bankszámlánkra kérhetjük az adott összeg kiutalását. • Online szerződéskötést és rendkívül gyors átvilágítást kínál, mint a bankok. Rendkívül gyors az integrálása is a legtöbb nagyobb e-kereskedelmi platform esetén.	• A vásárlók adatait és a vásárlási adatokat reklám célokra használja a Barion, majd eladja ezeket az adatokat, így aki nálunk vásárolt, annak más cég is hirdetni tud majd. Ha ezt ki szeretnénk kerülni, akkor 2% a jutalék. • A vásárlókat bosszanthatják a célzott reklámok, amelyet összekapcsolhatnak a kereskedővel, így az elveszítheti vevőinek egy részét. • Nem azonnal kapjuk meg a rendelések összegét a céges számlánkra, lehetnek akár hetes csúszások is.

• Többféle fizetési módot ajánl: ismétlődő, egy kattintásos, 3 szereplős, 2 lépcsős. A Barionon kívül csak az OTP tud még ilyen fizetési módokat ajánlani. • Csökkenti a kereskedő bankkártya visszaélésekből származó kockázatát, hiszen verifikált kártya esetén biztosítja a visszaélés elleni védelmet. • A vásárlók kijelző mérettől, operációs rendszertől és böngészőtől függetlenül bármilyen készülékről tudnak fizetni, mely kényelmet összekapcsolhatja a vásárló a kereskedővel.	• Magasabb lehet a vevők visszakozási aránya, hiszen a Barion kevésbé ismert, mint pl. az OTP, így bizalmatlanság léphet fel a fizetés biztonságával kapcsolatban. • A sikeres vásárlás után nem lehet egyedi „Köszönjük a vásárlást” oldalt beállítani, továbbá nem lehet a vevőket egy adott vásárlási útvonalon vezetni, ha további termékeket szeretnének eladni nekik, hiszen a vevő a Barion oldalán marad, ahol arra kéri, hogy regisztráljon magának Barion tárcát.
--	--

Forrás: SalesForm, 2021 (saját szerkesztés)

2014-ben a BankRáció (Money.hu, 2014) interjút készített a Barion társ-alapítójával: Bíró Tamással. Az interjú során Bíró Tamás megfogalmazta, hogy: „... a modellünk a Google biznisz modellje a pénziparban. Ilyen - tudomásunk szerint - még nincsen.” Manapság már számtalan vállalkozó hasonló modellben látja a lehetőséget. Boros Norbert (2019) blogbejegyzése szerint a rejtett bevétel modellben nem a fogyasztótól érkezik közvetlenül a bevétel, hanem valaki mástól. Erre az online hirdetések a legjobb példa, hiszen nem az olvasónak, hanem a hirdetőnek kell fizetnie, méghozzá a hirdetése után. Ezt a modellt követi a Facebook, a Google, illetve az online magazinok többsége. A modell problematikája azonban, hogy csak akkor éri meg egy harmadik félnek fizetnie, ha hatalmas az értékesítési volumen. A Barion társ-alapítója az előbb említett interjúban azt nyilatkozta, hogy: „Jelenleg közel 100 elfogadóhelyünk van, alapvetően Budapesten... Több mint 4.000 felhasználónk van már, ezekben több mint 10 millió forint e-pénzt bocsátottunk ki... E mellett 6.000 parkolóautomatánál is használható a Barion, ráadásul a nemzeti mobilfizetésben részt vevők közül a mi Android alkalmazásunkat értékelték a legtöbbször az ügyfelek: 4,4 a rátánk (Money.hu, 2014).” A Barion (2021) honlapjáról kiderül, hogy ma már több, mint 8000 vállalkozás használja a Bariont online fizetésre. Több, mint 2 500 000 Barion ügyfél és több, mint 8 000 Barion kereskedő van 20 EU országban. Az Androidos mobilapplikációjának viszont visszazuhant az értékelése 2,5-re. Véleményem szerint ez a versenytársakkal való összehasonlításból fakadhat, illetve az egyes ügyfelek számára zavarónak talált célzott hirdetésekre vezethető vissza.

Összefoglalva az eddigieket, a Barion a legígéretesebb hazai FinTech vállalkozások egyike, amely többféle FinTech tevékenységet is végez. PCI DSS tanúsítványának köszönhetően kétszereplős fizetési modellben is tud szolgáltatást nyújtani, az ügyfelek fizetési

adatainak védelme mellett. Elsőként vezette meg az erős ügyfélhitelesítést Magyarországon, és elsőként rendelkezett e-pénz licensszel is. Elektronikus pénzkibocsátási tevékenységének keretében saját tárcát üzemeltet, melyet összekötött egy FinTech-enabled marketplace modellel. Ennek során a szolgáltatást igénybe vevő kereskedők termékeket/szolgáltatásokat tudnak értékesíteni a vevőiknek, akik a Barion beépített fizetési kapujának segítségével, a regisztrált Barion tárcájukból tudnak fizetni. A hazai piacon működő többi digitális pénzügyi szolgáltatótól alacsony tranzakciós költségeikkel és díjaikkal, illetve adatmonetizációs tevékenységükkel differenciálják magukat.

Barion Pixel nevű opcionálisan implementálható eszközük segítségével kockázatelemzéshez és marketing tevékenységhez gyűjtenek adatokat, melyeket felhasználva jobban megismerhetik az ügyfelek szokásait és ezáltal személyre szabottabb szolgáltatást tudnak nyújtani. Látható tehát, hogy a Barion kihasználja a Big Data által kínált lehetőségeket. A különböző adatfeldolgozási és tárolási folyamatok (pl. rendszerben tárolt bankkártya számok, sütik segítségével begyűjtött ügyféladatokat) alapjaiban véve is visszaélési kockázatot hordoznak magukban. Az érzékeny pénzügyi-, és ügyféladatokat kiszivárgása az ügyfelek GDPR jogainak megsértése mellett visszaélésre ad lehetőséget a csalók számára. A Barion a kötelező érvényű szabályokat vezette be, melyek viszonylag magas csalásmegelőzési rátát biztosítanak, teljeskörű védelmet azonban így sem tud garantálni a vállalkozás. Az adathalászok az egyre kifinomultabb módszereinek köszönhetően még a magas biztonságú rendszerekbe is képesek betörni, így a kiberbiztonsági intézkedések folyamatos fejlesztése elengedhetetlen.

5.2. A FINTECHX TECHNOLOGIES ZRT. ESETTANULMÁNYA

A FintechX (4. táblázat) 2019-ben jött létre a lent látható 3 cég (Wyze, Aggreg8, FintechBlocks) összeolvadásával, melynek alapítói számos FinTech területen bemutatták már diszruptív ötleteiket. 2017 végén megtörtént az első kockázati tőkebefektetés a társaságban és 2018-ban az adataggregátor megoldásuk el is hozta számukra a FinTech Show győzelmet. Mivel az összeolvadás során létrejött vállalkozás megőrizte a fúzióban részt vevő vállalkozások önálló tevékenységeit, így az esettanulmány keretében a fúzióban részt vevő három vállalkozást külön-külön mutatom be.

4. táblázat: A FinTechX Technologies Zrt alapvető adatai

FintechX Technologies Zrt.			
Alapítás dátuma:	2019.11.25.	Nettó árbevétele:	88 750 eFt
Fő profilja:	Nyílt bankolás (open banking), pénzügyi adat aggregálás		
Wyze PFM Kft.	Aggreg8 Kft.	FintechBlocks Kft.	
2016.12.13.	2017.04.12.	2017.04.21.	
Költségkövető alkalmazás, márkanév nélküli FinTech alkalmazások fejlesztése	Pénzügyi adataggregátor, az első magyarországi számla-információs szolgáltató (AISP)	API-aggregátor megoldás, banki innovációs platform, a PSD2 megfelelést segíti	

Forrás: OPTEN, 2021 (saját szerkesztés)

A Wyze PFM Kft. FinTech start-up Magyarországon az első teljesen automatikus, bankfüggetlen személyes pénzügyi applikáció tulajdonosa, melynek missziója, hogy segítse a pénzügyi tudatosság elterjedését. A FinTechX Wyze.me applikációja a PSD2 nyílt bankolásra vonatkozó szabályainak köszönhetően számlainformációs szolgáltató (AISP – account information service provider) szerepbe lépett személyes pénzügyi menedzsment megoldásával. Az alkalmazás segítségével havi 5 perc időráfordítással egy interaktív diagram segítségével követhetjük nyomon a pénzügyeink alakulását. Az alkalmazásba csak 16 éven felüliek regisztrálhatnak, viszont annak használata teljesen díjmentes (Wyze.me, 2021). Az ingyenes regisztrációt követően tetszőleges számú bankszámla köthető a Wyze-hoz, amely automatikusan dolgozza fel a bankszámlánk tranzakciós adatait egy kliens oldali webscraping (weboldalakból adatkinyerés) technológiával. 9 magyar bank számlatörténetét lehet automatikusan – 1-2 perc alatt – szinkronizálni, a kinyert adatokat pedig egy teljes mértékben testre szabható, automatikusan tanuló algoritmus kategorizálja, hogy könnyen értelmezhetővé és átláthatóvá tegye a felhasználó számára a tranzakciók alakulását (Andor, 2016). A cég nevében a „PFM” az angol „personal finance management” (személyes pénzügyi menedzsment) kifejezés rövidítéséből származik, amely egy nemzetközileg elterjedt FinTech megoldás a személyes pénzügyek átláthatóbbá tételére, jellemzően valamilyen költségkövető alkalmazás keretein belül. Véleményem szerint az alkalmazás használatával nő a kockázata az érzékeny pénzügyi-, és ügyféladatok kiszivárgásának, ami megkönnyíti az adathalászok visszaélési és megtévesztési tevékenységeit. Az Android és iOS alapon is elérhető Wyze applikáció azonban nem olyan alkalmazás, amit csak úgy le lehet tölteni a mobiltelefonunkra.

Jelenleg a béta tesztelés lehetőségét is emailen keresztül kell kérni a cégtől, akik az email alapján hozzáadhatják az adott felhasználót a privát bétatesztelők listájához.

Az USA-ban és Nyugat Európában futó többi automatikus PFM megoldással ellentétben, amik szerver oldali szinkronizálást használnak, a Wyze kliens oldali szinkronizálást használ, melynek biztonságos használata érdekében a felhasználónak a Wyze plugint telepítenie kell a saját gépére. A Wyze szerint azért nem olyan biztonságos a szerver oldali szinkronizálás, mert akkor a PFM szolgáltató beékelődik a folyamatba, rajta keresztül folynak az adatok, így, ha a PFM szolgáltató szervereit feltörik, azzal minden felhasználó banki felhasználójához és jelszávához hozzáférhetnek. A Wyze plugin a letöltés után csatlakozik a felhasználó netbankjához, letölti annak bankszámlás tranzakcióit és anonimizálva feltölti azokat a Wyze felhő adatbázisába, majd kilép a netbankból. A felhasználó saját gépén megjegyzi a netbankos felhasználónevet és jelszót, így ezek nem szivárognak ki máshová. Szervereiken a regisztrált felhasználók esetében az alapvető számlainformációk (számlaszám, csomag neve stb.), a tranzakcióadatok (alapbeállításként az elmúlt 3 hónap adatai), a számlaegyenleg, illetve a netbanki elsőfaktoros belépési azonosítók kerülnek tárolásra. A Wyze.me-ben tárolt adatok az üzemeltető szerint a legmodernebb biztonsági intézkedésekkel kerülnek titkosításra. A felhasználó számítógépére letöltött adatok https alapú kapcsolaton keresztül kerülnek felküldésre a Wyze szervereire, még hozzá anonimizált módon, pl.: felhasználónév + tranzakció adatok (pl. kiskacs2, Vodafone, 10 000 Ft). Az anonimizálás akkor is védelmet nyújt, ha bárki feltörné a szerverüket, hiszen a hacker nem tudhatja, hogy a példában említett kiskacs2 tranzakciói kihez tartoznak. Ez azért lehetséges, mert a cég CRM rendszere, és ezáltal a felhasználók által megadott valós, vagy „maszkolt” identitása fizikailag is külön szerveren vannak, amik semmilyen formában nem érnek össze. A Wyze.me felhasználói felület üzemeltetője és fejlesztője az Aggreg8 Kft., így ő – illetve az őt felügyelő hatóság – garantálja az adatok védelmét. Az üzemeltető a Magyar Nemzeti Bank felügyelete alá tartozik, hiszen hivatalos számlainformációs szolgáltató (AISP) regisztrációját az MNB engedélyezte (Wyze.me, 2021). Mindezek ellenére a személyes meglátásom az, hogy a kiberbűnözés technológiai fejlettsége alkalmanként túllépi a védelmi intézkedések hatékonyságát. Ugyan az adatmentés a felhasználó gépére történik és titkosításra kerül, azonban arra nincs biztosíték, hogy a letöltési folyamatba ne ékelődhetne be egy adathalász.

A Wyze azért lehet ingyenes a felhasználók számára, mert a cég célja a banki aggregátor és kategorizálási algoritmusok optimalizálása, melyeket majd banki partnereiknek értékesítenek tovább (Wyze.me, 2021). Ezt megerősítendő, hogy a Wyze egyéb white-label FinTech alkalmazások fejlesztésével is foglalkozik, vagyis különböző márkázatlan FinTech

megoldásokat fejleszt ki és értékesít tovább más feleknek (pl. bankoknak). A BrandChannel (2018) szerint a white-label üzleti modell lényege, hogy a nagy szakértelemmel és kapacitással rendelkező gyártócégeknek nem kell marketingre költeniük, így kizárólag a termékek gyors és költséghatékony előállítására fókuszálhatnak. A márkázatlan termékeket értékesítik különböző cégeknek, akik aztán a saját logójukkal és csomagolásukkal felruházva forgalmazzák az adott termékeket a boltok polcain, így minden erőforrást az ötlet megvalósítására, a kreatív és hatékony márkáépítésre fordíthatnak, saját gyártási technológia- és infrastruktúra kiépítése nélkül. Véleményem szerint a gyors és hatékony fejlesztés miatt ennek az üzleti modellnek nagy a piaci potenciálja a FinTech szektorban.

A FinTechX aggreg8.io projektje egy pénzügyi adataggregátor megoldáson alapszik, amely a PSD2 által megnyitott banki adatvagyonhoz biztosít hozzáférést a szerződött üzleti partnereknek. Az Aggreg8 volt az első MNB által regisztrált számlainformációs szolgáltató (AISP) Magyarországon. Azóta az Aggreg8-en kívül 3 vállalkozás kapta meg az AISP engedélyét (Turzó, 2019): Appspect/Recash, Számlázz.hu, Zedna/Ginger App.

Az Aggreg8 Kft. számlainformációs szolgáltatóként három típusú szolgáltatást is elérhetővé tesz. Egy online felületen elérhető alkalmazás segítségével a felhasználó a bankszámláinak tranzakciótörténetét, illetve a közüzemi számlák számlázási információit egy felületre le tudja szinkronizálni, ezáltal a felhasználó gyorsan és egyszerűen átláthatja a pénzügyi helyzetét. A felhasználó a leszinkronizált adatokat meghozhatja az Aggreg8 üzleti partnereivel. Az Aggreg8 tehát bizonyos pénzügyi adatokat aggregál/összesít ügyfélfelhatalmazás alapján, majd az adatokat egységes formátumra hozza és egy standard API-n keresztül megoszthatóvá teszi (Aggreg8.io, 2021). A harmadik feles szolgáltatóként való beékelődés a folyamatokba meglátásom szerint a hálózatosodásból fakadó kockázatokat mutatja, hiszen az érzékeny információk több szereplőn futnak keresztül.

Az Aggreg8 TPP-státusszal (third party provider – harmadik feles szolgáltató) nem rendelkezők számára is nyújt banki adatokhoz való hozzáférést license-as-a-service megoldásuk segítségével. A PSD2 megnyitotta a bankok adatvagyonának egy részét új felek számára, azonban a szigorú szabályozás mellett helyi pénzügyi felügyeleti regisztrációra is szükség van, hogy hozzáférhessenek az adatokhoz. Az engedélyezési eljáráshoz átfogó szakismeretet és hatósági jártasság szükséges, nemzetközi tapasztalatok alapján a legfelkészültebb szereplők számára is több hónapos jelenleg a folyamat. Az Aggreg8.io olyan vállalkozásoknak kínálja a RegComp nevű szolgáltatását, akik ki szeretnék aknázni a PSD2 kínálta lehetőségeket, azonban az ehhez szükséges jogszabályi megfelelést nem saját erőforrást felhasználva kívánják teljesíteni. Az Aggreg8 a RegComp szolgáltatás keretében adott

vállalkozás, annak ügyfele és az Aggreg8 között háromszereplős szerződéses struktúrát képez, melyben:

- Az adott vállalkozás szeretné az ügyfelének banki számlainformációt felhasználni/beintegrálni az üzleti folyamataiba és/vagy termék-vagy szolgáltatás-nyújtásába (pl. könyvelés automatizálása, hitelbíráló, számlázó programok esetében a kiállított számlák teljesülésének nyomon követése stb.), ezért az Aggreg8 RegComp szolgáltatását veszi igénybe.
- Az Aggreg8 regisztrált AISP-ként jogosult az adott vállalkozás ügyfelének számlainformációihoz hozzáférni, de ahhoz előbb az ügyfélnek is szerződnie kell az Aggreg8-tel, hogy az adataihoz való hozzáféréshez engedélyt adjon.
- Ezt követően az ügyfél meghatalmazást ad az Aggreg8-nek arra vonatkozóan, hogy a megkapott banki számlainformációit megossza a RegComp szolgáltatást igénybe vevő vállalkozással egy információ-megosztási szolgáltatás keretében (Aggreg8.io, 2021).

Tehát a RegComp szolgáltatás során az Aggreg8 beékelődik a vállalkozás és annak ügyfele közé harmadik feles szolgáltatóként, hogy levegye a törvényi megfelelés terhét a vállalkozó válláról, akinek nem lenne joga közvetlenül hozzáférni az ügyfele banki tranzakciós adataihoz. Véleményem szerint rendkívül kockázatos tevékenység az, hogy az Aggreg8 olyan felek számára ad át banki ügyfél adatokat (az ügyfelek jóváhagyásával), amely vállalkozások nem rendelkeznek hatóságilag engedélyezett TPP-státusszal. Ezen banki adatok átadásának biztonságosságát egyrészt az Aggreg8 szubjektív megítélése jelenti a külső partnerrel való szerződéskötéskor, másrészt az ügyfél engedélye az adatok átadására. Az ügyfelek rálátása egy külső fél megbízhatóságára vonatkozóan meglátásom szerint közel sem teljeskörű, az Aggreg8 döntéseit pedig nagyban befolyásolhatja a bevételszerzés lehetősége.

Gémes Tamás a vele készített interjúban (Lemák, 2018) azt nyilatkozta, hogy: az Aggreg8.io-nak három nagy versenylőnye van a régióban hasonló megoldást nyújtó versenytársakkal szemben:

- Számos olyan pénzügyi adathoz is elérést biztosít, amelyek nem részei a PSD2-nek (pl. közmű számla adatok). Ezek az adatok nem csak nyers formátumban, hanem kategorizáltak is elérhetőek az Aggreg8.io gépi tanulás megoldásán keresztül.
- Szerződéses konstrukcióban nem csak az AISP regisztrációval rendelkező partnereknek szolgáltató az Aggreg8.io, hanem hamarosan már – regisztrált AISP szolgáltatóként – negyedik feles szolgáltatóknak is átadhat adatokat a GDPR előírásainak megfelelően.

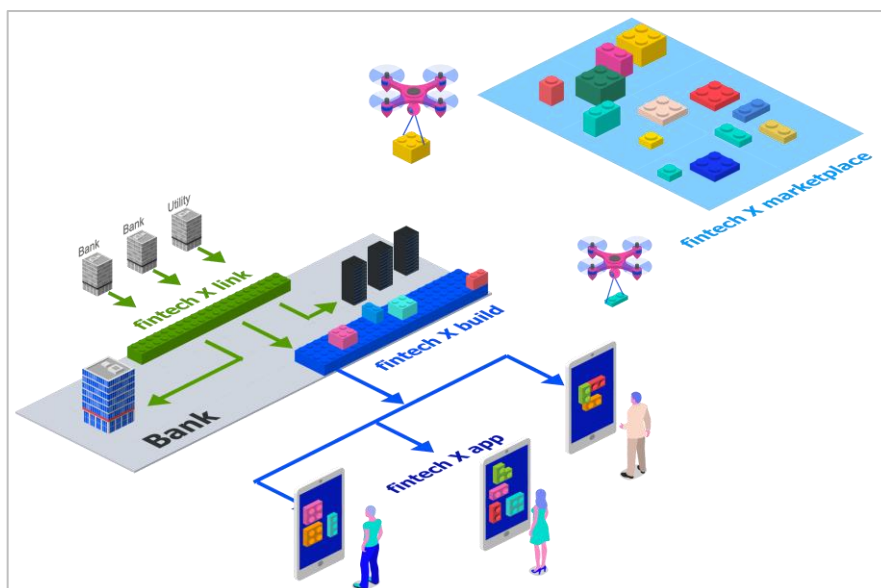
- Az Aggreg8.io-t publikus felhőben, valamint banki on-premise megoldás keretében is lehet telepíteni/futtatni, mely utóbbi a banki partnerek jogszabályi megfelelőségét segíti.

Mindezek mellett az ügyfeladatok biztonságát szem előtt tartva az Aggreg8.io a működését az MNB és egyéb hazai törvényi szabályozással, illetve az Európai Bankhatóság iránymutatásaival összhangban végzi. Ezek mentén a legerősebb biztonsági követelményeket is teljesíti, illetve megfelelő értékű szakmai felelősségbiztosítással rendelkezik (Aggreg8.io, 2021).

A FinTechX harmadik nagy ötlete a FinTechBlocks, amely banki API fejlesztésre és innovációs képesség javításra épül. Nyílt bankolási (open-banking) megoldásokat épít, melyek eredeti célja az volt, hogy a partnerei versenyképesekké váljanak és versenyképesek is tudjanak maradni a PSD2 szabályozás életbe lépése után is. A FinTechBlocks a bankok és a FinTech cégek közé készít egy olyan teret, amelyre bármelyik fél könnyen rá tud csatlakozni, amely gyorsabb és hatékonyabb kapcsolódást tesz lehetővé a FinTech cégek és a bankok rendszerei között, ezáltal könnyebb csomagban árusítani azok szolgáltatásait (Andor, 2017).

Az egyik alapító szerint (Andor, 2017), a FinTechBlocks platform-as-a-service egy piactér megoldás, ezért a bankok és a FinTech cégek számára egyaránt előnyös annak használata. A bankok a FintechBlocks rendszer implementációjával a PSD2 szabályozásból fakadó törvényi kötelezettségüknek is eleget tudnak tenni, illetve egy olyan gyorsan implementálható innovációs platformot kapnak, amely a jövőben is megállja majd a helyét. A későbbiekben a rendszer segítségével akár a belső fejlesztési projektjeiket, akár a külsős FinTech cégekkel történő együttműködésüket hatékonyabbá tudják majd tenni. A folyamat során a banki tűzfalon belül egy privát felhőt építenek ki, amely a banki core (központi) rendszerekhez kerül bekötésre. Ennek köszönhetően az integrált funkciók API-kon keresztül, felhőn belül és kívül is publikálhatók. A FinTech cégeknek azért javasolt a megoldás alkalmazása, mert egy FinTech és FintechBlocks közötti integráció kifejlesztésével minden olyan bank számára meg tudnak jelenni szolgáltatóként, akik bankként már integrálódtak a platformra (Lemák, 2018). Véleményem szerint a bankok és a FinTech vállalkozások együttműködésének segítése kiemelt fontosságú a hagyományos értékek megőrzése és a diszruptív technológiák terjedésének elősegítése szempontjából.

A FinTechX tulajdonosai a korábbi 3 cég/megoldás ötleteit egy egységbe/vállalkozásba foglalták (2. ábra), hogy a nyílt bankolással kapcsolatos szolgáltatások teljes spektrumát képesek legyenek lefedni. A FinTechX app-ot a Wyze, a FinTechX link-et az aggreg8 ötlete, a FinTechX build-et pedig a FinTechBlocks ötlete táplálja alapvetően (FinTech Group, 2020; FinTechX Technologies Zrt., 2021).



2. ábra: A FinTechX üzleti modelljének felépítése

Forrás: FinTechX Technologies Zrt., 2021

Összefoglalva az eddigieket, a FinTechX három rendkívüli ötletével vált a legígéretesebb FinTech cégek listájának szereplőjévé. A Wyze személyes pénzügyi menedzsment alkalmazása felhasználóbarát módon segít átlátni a pénzügyeket viszonylag kevés időráfordítás mellett. Azért lehet ingyenes a felhasználók (béta tesztelők) számára, mert a cég a banki aggregátor és kategorizálási algoritmusok optimalizálása után tovább értékesíti a terméket banki partnereik számára. Emellett a vállalkozás egyéb white-label fejlesztések keretében újszerű FinTech megoldások fejlesztésével és márkázatlan tovább értékesítésével foglalkozik. Az összeolvadásban résztvevő Aggreg8 volt az első MNB által regisztrált számlainformációs szolgáltató (AISP) Magyarországon. Az Aggreg8 nem csupán az ügyfél bankszámláinak tranzakciótörténetét, hanem a közüzemi számlák számlázási információit is képes leszinkronizálni egy felületre. TPP státusszal rendelkező vállalkozásként, RegComp nevű szolgáltatásának segítségével (license-as-a-service) a PSD2 szabályozás által kínált lehetőségek kiaknázásában segít olyan szolgáltatóknak, akik az ehhez szükséges jogszabályi megfelelést nem saját erőforrást felhasználva kívánják teljesíteni. A fúzió harmadik résztvevője a FintechBlocks, amely a bankok és a FinTech cégek közé készít egy olyan piactér jellegű megoldást (platform-as-a-service), amelyre bármelyik fél könnyen rá tud csatlakozni, így gyorsabb és hatékonyabb a kapcsolódás a FinTech cégek és a bankok rendszerei között. A rendszer implementációjával a bankok PSD2-ből fakadó törvényi kötelezettségüknek is eleget tudnak tenni. Adatfeldolgozás tekintetében a FinTechX a gépi tanulást és egyéb mesterséges intelligencián alapuló megoldást alkalmaz.

A Wyze költségkövető alkalmazása érzékeny pénzügyi ügyfeladatokkal dolgozik, ezek kiszivárgását pedig egy szerver oldali szinkronizálással védi ki. Ez az alapító bevallása szerint sokkal biztonságosabb, mint a nyugati országok bevett gyakorlata, azonban arra nincs biztosíték, hogy a letöltési folyamatba ne ékelődhetne be egy adathalász. Az Aggreg8 regisztrált AISP-ként jogosult a banki ügyfelének számlainformációihoz hozzáférni – azok előzetes engedélyével –, így harmadik feles szereplőként plusz eleme az információs hálónak, mely hálózatosodás a szakirodalmi források alapján kockázatot hordoz magában. Véleményem szerint rendkívül kockázatos tevékenység az, hogy az Aggreg8 olyan felek számára ad át banki ügyfél adatokat RegComp szolgáltatásának keretein belül (az ügyfelek jóváhagyásával), amely vállalkozások nem rendelkeznek hatóságilag engedélyezett TPP-státusszal. Ezen banki adatok átadásának biztonságosságát egyrészt az Aggreg8 szubjektív megítélése jelenti a külső partnerrel való szerződéskötéskor, másrészt az ügyfél engedélye az adatok átadására. A FintechBlocks felhőalapú platform szolgáltatással foglalkozik, amely alapvetően kockázatosnak számítana, azonban a folyamat során a banki tűzfalon belül egy privát felhőt építenek ki, amely a banki központi rendszerekhez kerül bekötésre, így nem publikus felhőről beszélünk, ami egyfajta belső banki magánhálózatként értelmezhető. Annak viszont, hogy belső banki hálózatról ne kerüljenek publikus felületekre-, illetve magáncélú felhasználásra az adott adatok, csak a banki dolgozók etikus és jogkövető magatartása szab gátat.

5.3. A SEON TECHNOLOGIES KFT. ESETTANULMÁNYA

Az online bankkártyás fizetés elterjedésével párhuzamosan nő a csalások és visszaélések száma is. A jelenlegi szabályozás szerint a bankkártyás fizetési csalásokért a kereskedők felelnek, így, ha visszaélés történik, akkor a kereskedő köteles visszatéríteni a vásárlás összegét a bankkártya tulajdonosának, még akkor is, ha az árut már kiszállították a csaló számára (FINTECHZONE, 2017).

A SEON (5. táblázat) számos iparág számára kínál csalás-detektáló megoldásokat: bank és biztosítás, online játék és szerencsejáték, online hitelezés, e-kereskedelem, utazás és jegyértékesítés, fizetési kapuk, kriptovaluta és kereskedelem. Minden iparágra vonatkozóan az adott célnak megfelelő, testreszabott megoldást biztosít. Az imént említett iparágak közül én kizárólag a pénzügyekkel kapcsolatos területeket veszem górcső alá. Pénzügyi vonalon a SEON egy olyan csalásmegelőző rendszert fejleszt, amely gépi tanulás segítségével szűri ki a lehetséges csalásokat az online tranzakciók során. Ügyfelei közé tartozik többek között az OTP- és a Gránit Bank, valamint a Barion is.

5. táblázat: A SEON Technologies Kft. alapvető adatai

SEON Technologies Kft.			
Alapítás dátuma:	2017.01.10.	Nettó árbevétele:	504 819 eFt
Fő profilja:	Online bankkártyás fizetések és autentikációs pontok kockázatelemzése		

Forrás: OPTEN, 2021 (saját szerkesztés)

A SEON a 2017-ben megrendezett FinTech show-n mutatta meg először magát nagyközönség előtt. 2018 februárjában már 150 millió forintnak megfelelő tőkebefektetést kapott az OTP Csoporthoz tartozó Portfolion és a Friedler Capital társaságoktól, majd 2019-ben a Portfolion újabb 1 millió eurót fektetett a társaságba. 2019-ben startup díjat nyertek az európai Lendit konferencián ("Pitch-it"), a 2020-as G2 Crowd platformon pedig "leader" kitüntetést kaptak a fraud protection (csalásmegelőzés) kategóriában, 2020-ban pedig már Londonban is irodát nyitottak (FINTECHZONE, 2021).

A FinTech megoldásuk célpiacának elsődlegesen a pénzintézetek tekinthetők, de más vállalkozásokkal (pl. Barion) is partnerséget kötöttek már. BigData alapú megoldásuk segítségével a kiberbiztonság szegmensén belül online pénzforgalmi ügyletekhez kapcsolható kártyacsalás-detektálással, illetve felhasználói nevekkel történő visszaélések (pl.: adathalászat) azonosításával foglalkoznak. Újszerű megközelítésüknek köszönhetően az elektronikus ügyfélazonosítást (KYC – Know Your Customer) egyszerűbbé és biztonságosabbá tették a szolgáltatást igénybe vevők számára, ami pénzintézetek esetében például az ügyfelek net/mobilbanki azonosítását takarja. Az online hitelezésre kialakított csalás-detektáló eszközük segít elkerülni a nemteljesítő ügyféllel való problémákat és ellenőrzi, hogy az adós valóban az-e, akinek mondja magát. Bankok és biztosítótársaságok esetében a SEON segíti az ügyfelet a legújabb szabályoknak és irányelveknek való megfelelésben, például az erős ügyfélhitelesítés területén. A kriptovaluták és devizaügyletek esetében segít megakadályozni, hogy a csalók lopott személyazonossággal tudjanak pénzt átváltani, vagy felvenni. A lopott, vagy mesterségesen generált személyazonossággal belépőket azonnal blokkolja a rendszer, az adathalászokat pedig hamar leleplezi (T-Systems, 2016; FinTech Group, 2021, SEON Technologies Kft., 2021).

A SEON fizetési kapukra formált megoldása adott vásárlás kapcsán több szempont alapján elemzi az elérhető információkat, majd ezek alapján levonja a következtetéseit a visszaélés esélyére vonatkozóan. A rendszer vizsgálja az eszköz IP címét, a földrajzi helyet,

illetve ellenőrzi az eszközt is, amelyről a vásárlást indították. Értékeli a vásárló e-mail címét, ez alapján vizsgálja a közösségi médián elérhető profil információkat, elemzi a felhasználói viselkedését, majd mindezeket összeveti a kártyatulajdonos korábbi online viselkedésének mintázatával (SEON Technologies Kft., 2021). Összességében tehát a csalásmegelőző rendszerükben az adatgyűjtés során felépítenek egy kockázati profilt, amit a rendszer a meglévő adatokból kiindulva, különböző publikus és közösségi forrásokból bővít ki egy teljes kockázati profillá (FinTech Group, 2021).

A kockázatelemzés során egy adott tranzakció azonnal besorolásra kerül a gépi tanulás modellek alkalmazásával, de a döntési folyamat mindeközben teljesen átlátható marad. A kockázat pontozása, illetve szintjének megállapítása során vannak előre meghatározott szabályok, amelyek a meglévő iparág-specifikus adatokon alapszanak, de a felhasználó tud új – esetleg cégspecifikus – szabályt is hozzáadni a rendszerhez. A gépi tanulás is hoz létre új szabályokat, amelyek beépítését a felhasználó hagyja jóvá. A kockázati pontozás során az imént említett szabályok hozzáadnak, vagy levonnak kockázati pontot az adott esetre vonatkozóan, majd kialakul egy pontszám, amely 0–100-ig terjedhet, ahol a 0 a kockázatmentes és a 100 az extrém kockázatos szint. Az online fizetés lebonyolítása során, amennyiben a rendszer – a felhasználó beállításai alapján – nagynak ítéli meg a csalás valószínűségét, úgy automatikusan blokkolja a tranzakciót. Kisebb csaláskockázat esetén a kereskedő kap egy e-mailt a gyanús vásárlási kísérletről, ilyenkor javasolt például telefonon – mint másik csatorna – keresztül megbizonyosodnia a cégnek arról, hogy valóban a kártya tulajdonosa próbált-e meg fizetni a bankkártyával (SEON Technologies Kft., 2021). Meglátásom szerint a kritikus döntéshozatal kapcsán alkalmazott AI technológiák a gyorsaságon és hatékonyságon túl felvethetik a kontroll elvesztésének lehetőségét, vagy annak hatékonyságának romlását.

A SEON-nak a fent említett tevékenységek kivitelezésére alapvetően két terméke van, melyek a csalásmegelőzés hatékonysági szintjében térnek el egymástól. A termékek pontos működésének megértéséhez mélyebb informatikai magyarázatra lenne szükség, amit jelen dolgozatban nem fejtek ki. Az egyik termék neve az „Intelligence Tool”, amely széleskörű adatgazdagítást használva segíti a csaláskezeléssel kapcsolatos döntéshozatalt, a manuális tranzakció ellenőrzéseket szinte teljesen automatizálva. Az adatgazdagítás folyamatában a rendszer összegyűjti az összes, nyilvánosan elérhető adatpontot a vizsgált személy digitális lábnyomáról. Ennek a terméknek 3 modulja van, amelyek IP cím, email cím és telefon (mint eszköz) vizsgálatot végeznek. Az „Intelligence Tool” tulajdonképpen egy Chrome bővítményként működik, így nem szükséges integrálni sem. A másik termék neve a „Sense Platform”, amely az előző termékkel ellentétben egy teljeskörű csalás-menedzsment rendszert

foglal magában. Szoftver- és hardver konfiguráció segítségével elemzi a vizsgált alanyok online magatartását, illetve elemzi a belépés során használt eszköz digitális ujjlenyomatát. Számos egyéb forrás mellett a közösségi média profilokat is felhasználja, hogy valós időben gazdagítsa a megszerzett adatokat. Ezt a terméket kb. egy órába kerül integrálni – teljesen ingyenesen – és amint üzemkész állapotba kerül, azonnal csökkenti a tranzakciós visszaélések számát. Gépi tanulás segítségével a korábban detektált csalási esetekből tanulva a rendszer folyamatosan növeli a saját hatékonyságát, de a felhasználó egy API-n keresztül szinte mindent testre szabhat.

A SEON mindkét termékéről részletes leírást tesz közzé a honlapján, számos infografika, e-könyv, podcast és egyéb eszköz segítségével igyekszik megértetni a termékeinek működését a jövőbeli ügyfelekkel. A termékek árazása és a kifizetésük módja azonban szintén eltérő módszert követ. Az „Intelligence Tool” esetében többszintű árképzést alkalmaznak, tehát különböző csomagok közül kell választani, amelyeknek eltérőek az áraik, a legkisebb csomag ára 99€/hónap. A termék tesztelésére egy 7 napos ingyenes használati periódust ajánlanak fel. A „Sense Platform” esetében használat alapú árazási politikát követnek, vagyis minden egyes átnézett tranzakció után számolnak fel néhány centet, a legkisebb összegű számla 6 cent lehet. Az összegyűlt összeget pedig következő hónap elején számlázzák ki, vagyis mindig az adott ciklus végén kell fizetni, amely átutalással és bankkártyával is rendezhető. Ebben az esetben a SEON egy 30 napos ingyenes próbaverziót bocsát az ügyfél rendelkezésére. Mindkét termék esetében elegendő egy előfizetés, a rendszerhez való hozzáférés megosztható a munkatársak között, illetve személyre lehet szabni a hozzáférés típusához kapcsolódó jogosultságokat is (SEON Technologies Kft., 2021). A csalásmegelőző termék beépítése a folyamatba meglátásom szerint a hálózatosodásból fakadó kockázatokat mutatja, hiszen az érzékeny információk több szereplőn futnak keresztül. Az érzékeny pénzügyi-, és ügyféladatok kiszivárgása hatalmas károkat okozhat. A kockázat megítélési paraméterek – minimálisan – személyre szabhatók, így véleményem szerint kis mértékben manipulálhatók is. A tranzakciót kockázatosnak minősítő küszöbérték fentebb állíthatósága meglátásom szerint lehetőséget ad arra, hogy az eszközt felhasználók manuálisan „átengedjék” a csalókat az ellenőrzésen.

A Barion és a SEON megállapodást kötött, hogy hatékonyabban tudjanak fellépni az online kártyás fizetések során tevékenykedő kibercsalókkal szemben. A SEON csalás-detektáló eszközét beépítették a Barion fizetési rendszerébe, ami így a kártyás visszaélési kísérletek közel 80%-át már képes kiszűrni. Az eszköz beépítését megelőzően a Barion alkalmazottai manuálisan próbálták kiszűrni a gyanús tranzakciókat a szokásos munkaidőben, így az esti és hétvégi gyanús tranzakcióknak „várakozniuk” kellett. Hamar bebizonyosodott, hogy a folytonos lemaradás nem fenntartható egy olyan online piacon, ahol 24/7 történnek a

tranzakciók. A vállalkozás növekedéséhez is elengedhetetlen volt, hogy a csalások számát olyan alacsonyan tartsák, amennyire csak lehetséges. A Barion számára rendkívül megnyerő volt a SEON UX és UI dizájnya, csalás-detektáló eszközének beiktatásával pedig azonnal látszódtak annak előnyei. A gépi tanulásnak köszönhetően egy napról napra egyre jobb csalás-kiszűrő rendszerrel gazdagodott a Barion (Kiss, 2021b). A UX dizájn az angol “User Experience design” rövidítése, mely magyarul a felhasználói élményt jelenti. Ez a benyomás keltés művészete, melynek célja, hogy a felhasználó kényelmesen érje el a céljait az adott felületen. A UI a felhasználói felület (User Interface) vizuális kialakítását jelenti, melynek elsődleges célja, hogy a tartalmat és a már meglévő szerkezetet vonzó módon tálalja a felhasználók számára (Digital Natives, 2021).

Összegezve a fentieket, A SEON csalásmegelőző rendszert épített, melyet két – eltérő mélységben elemző – csalás-detektáló eszköz formájában kínál a felhasználók számára. Az adatgyűjtés során felépítenek egy kockázati profilt, amit a rendszer a meglévő adatokból kiindulva, különböző publikus és közösségi forrásokból bővít ki egy teljes kockázati profillá. A kockázatelemzés során egy adott tranzakció azonnal besorolásra kerül a gépi tanulás modellek alkalmazásával. A teljeskörű csalás-menedzsment rendszerük elemzi a vizsgált alanyok online magatartását, illetve a belépés során használt eszköz digitális ujjlenyomatát. Valós időben gazdagítja az adatokat többek között a közösségi média profilokat felhasználva. Az összetettebb eszközt szükséges csak integrálni, amely rendkívül gyorsan elvégezhető és élesítést követően azonnal csökkenti a tranzakciós visszaélések számát.

A Barion fizetési kapujára alkalmazott SEON megoldás a kártyás visszaélési kísérletek közel 80%-át képes kiszűrni. Gépi tanulás segítségével a korábban detektált csalási esetekből tanulva a rendszer folyamatosan növeli a saját hatékonyságát, emellett a felhasználó egy API-n keresztül szinte mindent tesztre szabhat (pl. jogosultságokat, kockázati besorolási küszöbértékeket stb.). A SEON kockázatmegelőzéssel foglalkozó vállalkozás, azonban így is hordozhat a működése némi kockázatot. Véleményem szerint, azáltal, hogy az eszközük beépül a tranzakciós folyamatba, a hálózatosodás szakirodalmi háttérét tekintve egy újabb kockázati pontot testesítenek meg, hiszen az érzékeny információk így több szereplőn futnak keresztül. Az érzékeny pénzügyi-, és ügyféladatok kiszivárgása pedig hatalmas károkat okozhat. A csalásdetektáló eszközök kockázat megítélési paraméterei – minimálisan – személyre szabhatók, így véleményem szerint kis mértékben manipulálhatók is. Ezáltal fentebb állítható az a küszöbérték, amely esetén a tranzakciót végrehajtó kockázatosnak minősül, ami meglátásom szerint lehetőséget ad arra, hogy az eszközt felhasználók manuálisan „átengedjék” a csalókat az ellenőrzésen.

5.4. A BANKMONITOR KFT. ESETTANULMÁNYA

A folyamatos digitalizáció miatt megnőtt az igény a pénzügyi termékek kínálatának átláthatóságára és összehasonlíthatóságára is. Mindezt az ügyfelek gyorsan szeretnék elintézni, így a legegyszerűbb megoldás az, ha a különböző szolgáltatók termékeit egy felületen láthatja az ügyfél. FinTech Group (2020) szerint a Bankmonitor (6. táblázat) egy klasszikus piactér logika mentén, digitális ügynöki megközelítéssel ékelődött be a hagyományos – bankok és ügyfelek közötti – értékesítési láncba, hogy segítse a fogyasztókat az olyan pénzügyi termékek gyors megtalálásában, amelyek a lehető legjobban illeszkednek az egyéni igényeikhez. Célpiaça a lakossági és kkv piac, valamint ügynöki tevékenysége által a pénzügyi szolgáltatók.

6. táblázat: A Bankmonitor Kft. alapvető adatai

Bankmonitor Kft.			
Alapítás dátuma:	2011.12.14.	Nettó árbevétele:	267 438 eFt
Fő profilja:	Hitel/betéti konstrukciók összehasonlítását, kiválasztását segítő platform		

Forrás: OPTEN, 2021 (saját szerkesztés)

A bankmonitor.hu oldalon adatkezelő a Bankmonitor Szolgáltató Kft., Bankmonitor Kft., Bankmonitor Partner Kft., mely társaságok eltérő tevékenység végzésére jogosultak. Maga a honlap és az üzemeltetéséhez kapcsolódó jogok a Bankmonitor Kft.-t illetik, a honlapot szolgáltatás nyújtás céljából pedig a másik két társaság veheti igénybe. A Bankmonitor Szolgáltató Kft. jelenleg nem végez a honlapon megjelenő pénzügyi és biztosítási szolgáltatásokhoz kapcsolódó tevékenységet, mert ez a társaság a Concorde Alapkezelő Befektetési Alapkezelő Zrt. tőkepiaci függő ügynöke. A Bankmonitor Kft. a honlapon található pénzügyi és befektetési termékekhez kapcsolódó marketing tevékenységet végez (pl. „Promóció” jelzésű termékmegjelenítés, bannerek). A honlapon található bizonyos termékekkel kapcsolatos közvetítői, többes ügynöki, biztosítás közvetítői, tagszervezői tevékenységeket a Bankmonitor Partner Kft. végzi az MNB felügyelete alatt. A bankmonitor.hu honlap célja, hogy valamennyi termékkategóriában vagy a legnagyobb piaci szereplők, vagy az adott termékkategória legmeghatározóbb szereplői kerüljenek megjelenítésre. Előfordulhat, hogy a honlapra látogató felhasználó a kalkulátorokban, illetve a találati listákban talál olyan termékeket is, amelyek közvetítésére nem jogosult egyik Bankmonitor társaság sem. Ezen

termékek megjelenítése a felhasználó szélesebb körű tájékoztatását szolgálja (Bankmonitor Kft., 2021).

A bankmonitor.hu tulajdonosi köre bankoktól teljesen független, magyar magánszemélyekből áll, így az objektivitásuk ilyen szempontból is biztosított. Az egyes termékek feltüntetésekor sem befolyásoló tényező a banki érdek, ha egy találati listában az első helyen szerepel egy adott bankbetét, vagy bankszámla, akkor az a keresési szempontok és a futtatott algoritmus alapján a legkedvezőbb termék. A bankoknak természetesen lehetőségük van kiemelni a terméküket a bemutatáskor bizonyos ellenérték fizetésének ellenében, de a Bankmonitor azt az adott terméket „fizetett hirdetés” címkével jelöli meg (Bankmonitor Kft., 2021). Véleményem szerint kockázati tényező lenne, ha a Bankmonitor által garantált objektivitás megsérülne, hiszen ennek a hazai viszonylatban meghatározó platformnak az esetleges szubjektív, vagy egyéb érdekek által vezérelt javaslatai nagyban tudnák befolyásolni az ügyfelek pénzügyi választásait.

Lakossági és vállalati termékek összehasonlítására egyaránt kínálnak lehetőséget, majd a legjobb személyre szabott ajánlat megtalálása után szerződéskötésig segítik az ügyfelet. Ez egy olyan end-to-end (E2E) megoldás, amivel vezető szerepet töltenek be a hazai bankfüggetlen szolgáltatók között. A Bankmonitor saját fejlesztései között megtalálható a valós idejű nyomon követés, okos hitelképesség bírálat, saját CRM rendszer és digitális ajánlatadó rendszer (Bankmonitor Kft., 2021).

A fejlesztések finanszírozására 2013 első felében, majd ezt követően két további finanszírozási körben az Euroventures IV. alap fektetett a társaságba Kovács Zoltán társbefektetővel egyetemben. 2015-ben stabilizálták a cég üzleti modelljét és 2017 óta folyamatosan foglalkoznak FinTech fejlesztésekkel a megtermelt profit visszaforgatásán keresztül (Domokos, 2021). Fejlesztéseik során elsődleges szempont a folyamatos digitalizáció és a maximális ügyfélélmény biztosítása. Ezek kiemelt fontosságúak a FinTech szektorban, hiszen ezen tényezők testesítik meg a fogyasztók elsődleges döntési kritériumait a digitális pénzügyi szolgáltatók megválasztásakor.

Piaci részesedésének növelése mellett 50 százalékkal növelte meg az árbevételét a 2020-as évben. A Bankmonitor Kft. ingyenesen használható online platformján keresztül a saját fejlesztésű kalkulátoruknak segítségével ma már több, mint 30 bank és egyéb pénzügyi szolgáltató több ezer termékét lehet összevetni. A bankpiac kínálatának 95%-a megtalálható a bankmonitor.hu-n és havonta 350.000 ezren használják a weboldalt általános pénzügyi tájékozódásra, vagy pénzügyi termékek összehasonlítására, amivel Magyarország legnagyobb banki termék összehasonlító weboldalává nőtte ki magát a bankmonitor.hu. Minden szegmens

esetében törekednek a termékfeltételek átláthatóbbá tételére, aktuális hírekkel és szakmai tartalmakkal is segítik az ügyfeleket az objektív döntéshozatalban. Ezt a folyamatot több, mint 15 független pénzügyi szakértő támogatja legalább 5-20 éves tapasztalattal (Bankmonitor Kft., 2021). A fent látható adatokból is hangsúlyosabbá válik a Bankmonitor fogyasztókat befolyásoló hatása azok pénzügyi döntéseinek meghozatalakor.

A több ezer banki termék feltételeinek dzsungelében az összehasonlító felületekkel és kalkulátoraikkal segítenek a felhasználóknak eligazodni. A weboldalukon megtekinthető lakossági banki termékek kiterjedt adatbázisát az alábbi kategóriákra osztják: lakáshitel, személyi kölcsön, babaváró hitel, bankszámla, hitelkalkulátor, hitelkiváltás, nyugdíj megtakarítás, Széchenyi hitel. A felhasználó minden kategóriában talál egy rövid leírást az adott témakör alapvető jellemzőiről, majd a Bankmonitor bankfüggetlen piaci szereplőként kínál fel ajánlatokat a felhasználónak online formában. A személyi kölcsönre és babaváró hitelre a teljes hitelcsomag összeállítható online, ami a pozitív banki elbírálást követően közvetlenül szerződhetővé válik, mely digitális megoldást a jelzáloghitelekre is ki akarják terjeszteni. A személyi kölcsön folyósítása és a bankszámlanyitás már teljes mértékben digitálisan intézhető (Bankmonitor Kft., 2021). A weboldal rendkívül felhasználóbarát, a sok infografikának és szakmai magyarázatnak köszönhetően nem csak a pénzügyi végezethez szükséges tudják könnyen értelmezni a feltüntetett információkat. Ennek – a magas ügyfélélmény megteremtése mellett – kiemelt fontossága van a pénzügyi tudatosság fejlesztésének kapcsán.

2019. január 1-jétől a jogszabályok megengedik, hogy a bankok közvetett ügyfél-átvilágítással azonosítsák az ügyfeleiket. Így nem valós időben, például egy selfie videó vagy kép beküldésével, az azonosítóokmányok befotózásával, illetve a megfelelő adatok elektronikus megadásával lehet bankszámlát nyitni. A Bankmonitorral együttműködésben a hazai pénzintézetek között a CIB Bank volt az első, aki egész nap elérhető online folyamattal is kínál bankszámlanyitást ügyfelei számára. A szolgáltatás keretében az ügyfél a bankmonitor.hu oldalon keresztül tud kedvezményes CIB ECO bankszámlát igényelni elektronikus szerződés aláírás segítségével. Az igénylést a bank ellenőrzi és ha azt jóváhagyja, akkor a következő munkanapon meg is nyitja a bankszámlát (FINTECHZONE, 2020).

A Bankmonitor a honlapján feltüntetett üzleti szabályzatában kiemeli, hogy többes ügynöki szereplőként van jelent a hazai pénzügyi piacon, mely tevékenységét kizárólag a Magyar Nemzeti Bank engedélyével végezheti. A többes ügynök olyan független közvetítő, amely több pénzügyi intézmény egymással versengő pénzügyi szolgáltatásának vonatkozásában pénzügyi szolgáltatás közvetítését végzi. A Bankmonitor esetében ez magában foglalja a pénzügyi intézményekkel kötött megbízási szerződés alapján pénzügyi szolgáltatás,

kiegészítő pénzügyi szolgáltatás nyújtásának, illetve ilyen szolgáltatásra irányuló szerződés megkötésének elősegítésére irányuló tevékenységet. Ennek során a Bankmonitor a pénzügyi intézmény kockázatára önállóan kötelezettséget nem vállal, szerződést nem köt és hiteltanácsadási tevékenységet sem végez. A Bankmonitor az ügyféllel való kapcsolata során a tudomására jutott banktitoknak minősülő információkat a jogszabályi előírásoknak megfelelően banktitokként kezeli, és azt időkorlátozás nélkül, az üzleti kapcsolatok megszűnése után is megőrzi. Az üzletszabályzatban azt is leírja a Bankmonitor, hogy az ügyfél és a Bankmonitor között létrejövő közvetítői szerződés célja – többek között –, hogy az ügyfél részére legalább három pénzügyi intézmény egymással versengő pénzügyi szolgáltatását elemezze és átadja, amennyiben ez a mennyiség a piacon hozzáférhető (Bankmonitor Kft., 2021). Véleményem szerint hatalmas kockázatot jelent, hogy a Bankmonitor külső szolgáltatóként banktitoknak minősülő adatokat is kezel, hiszen ezek kiszivárgása visszaélésre és megtévesztésre adna lehetőséget a csalók számára.

A weboldalt látogatók számára azért lehet ingyenes a Bankmonitor szolgáltatása, mert a bevételeinek túlnyomó része a bankoktól származik. A Bankmonitor a pénzügyi intézményekkel (pl. bank) köt megállapodásokat, melyek keretében az egyes termékek iránti érdeklődések az intézmény számára átadásra kerülnek. Ezen felül számos olyan feladatot végez, ami eredetileg egy bankfiók tevékenységi körébe tartozna, így az ügyfélszolgálással költséget takarít meg a bankoknak, amely költségmegtakarításból részesedik a Bankmonitor. Ügyféltől származó közvetítői díjra nem jogosult a Bankmonitor, közvetítői díjat kizárólag a megbízó pénzügyi intézménytől fogadhat el. Ugyanakkor, ha az ügyfél számára más – a pénzügyi szolgáltatás közvetítésének nem minősülő – szolgáltatást is nyújt, akkor megengedett, hogy annak ellenértékeként díjat számítson fel. A Bankmonitor csupán ajánlatokat hasonlít össze, őt meg nem illető pénz nem folyik keresztül rajta. Így az ügyfél nevében a megbízó pénzügyi intézménytől az ügyfelet megillető pénzt nem veszi át, és az ügyfél által fizetendő, a megbízó pénzügyi intézményt megillető pénzösszegeket sem (Bankmonitor Kft., 2021). Meglátásom szerint a FinTech szektorban működő vállalkozások piaci pozíciója szoros összefüggésben van az ügyfélélménnyel, aminek része az árazás. Éppen ezért az ügyfél számára ingyenes szolgáltatásnyújtás – melynek háttérében persze vannak bevételek – rendkívül hatékony módja a nagyszámú fogyasztói réteg megszerzésének, ezáltal egy nagyobb piaci részesedés elérésének.

Fontos kiemelni, hogy az ügyfél kérésére a Bankmonitornak tájékoztatást kell adnia arról, hogy mennyiben tér el egymástól az ügyfélnek kínált hiteleket nyújtó pénzügyi intézmények által fizetendő díjazás mértéke. Az ügyfelet kötelező arról is tájékoztatni, hogy jogosult ilyen

információt kérni. A Bankmonitornak a tevékenységéből eredő károk biztosítására káreseményenként legalább 460.000 EUR, évente együttesen pedig legalább 750.000 EUR összegű felelősségbiztosítása áll rendelkezésre (Bankmonitor Kft., 2021). Fontos megjegyezni ugyanakkor, hogy az érzékeny adatok kiszivárgásának kárai az imént említett összegek többszörösét is kitehetik.

A weboldal sütiken (cookie) keresztül, egyedi azonosítására alkalmatlan, nem személyhez kapcsolódó statisztikai adatokat is gyűjt remarketing és a honlap fejlesztése céljából. Ezen felül a sütik azt is nézik, hogy a felhasználók hogyan használják a weboldalt, ott milyen tevékenységet végeztek, hogy még inkább releváns ajánlatot tudjanak küldeni az ügyfélnek. Ügyfélélményt támogató megoldás, hogy a korábban felkeresett kalkulátorok paramétereit is elmenti a rendszer, hogy az oldalra visszatérve a felhasználó ott folytathassa a keresést, ahol korábban abbahagyta. A személyhez nem köthető összességű adatok külső felek részére továbbításra kerülhetnek. Érdekes információ, hogy a marketing és remarketing célú átadás esetén lehetséges, hogy a külső harmadik fél (pl. Facebook, Google) mégis képes beazonosítani az ügyfelet ezen adatok alapján és így személyre szabott szolgáltatásokat nyújthat neki (Bankmonitor Kft., 2021).

Összefoglalva az eddigieket, a Bankmonitor egy klasszikus piactér logika mentén, digitális ügynöki megközelítéssel ékelődött be a hagyományos – bankok és ügyfelek közötti – értékesítési láncba. Lakossági és vállalati termékek összehasonlítására összehasonlító felületekkel és kalkulátoraikkal segítenek a felhasználóknak, majd a legjobb személyre szabott ajánlat megtalálása után szerződéskötésig segítik az ügyfelet. Ez egy olyan end-to-end (E2E) megoldás, amivel vezető szerepet töltenek be a hazai bankfüggetlen szolgáltatók között. Tulajdonosi köre bankoktól teljesen független, magyar magánszemélyekből áll, így az objektivitásuk ilyen szempontból is biztosított. A weboldalt látogatók számára azért lehet ingyenes a Bankmonitor szolgáltatása, mert a bevételeinek túlnyomó része a bankoktól származik. A Bankmonitorral együttműködésben a hazai pénzügyintézetek között a CIB Bank volt az első, aki egész nap elérhető online folyamattal is kínál bankszámlanyitást ügyfelei számára. Elektronikus és teljes mértékben automatizált szolgáltatásaik közül kiemelendő, hogy weboldaluk használatának segítségével a személyi kölcsönre és babaváró hitelre a teljes hitelcsomag összeállítható online. Ezek a pozitív banki elbírálást követően közvetlenül szerződhetővé válnak, mely digitális megoldást a jelzáloghitelre is ki akarják terjeszteni. A személyi kölcsön folyósítása és a bankszámlanyitás pedig már teljes mértékben digitálisan intézhető. A Bankmonitor a honlapján személyhez kapcsolódó statisztikai adatokat gyűjt sütik segítségével remarketing és a honlap fejlesztése céljából. A korábban felkeresett kalkulátorok

paramétereit is elmenti a rendszer, hogy az oldalra visszatérve a felhasználó ott folytathassa a keresést, ahol korábban abbahagyta. Jól látszik tehát, hogy a Bankmonitor a Big Data előnyeit kiaknázva igyekszik minél magasabb ügyfélélményt nyújtani a felhasználóinak. Véleményem szerint kockázati forrás, hogy az ügyfelek begyűjtött – személyhez nem kapcsolható – adatai a marketing és remarketing célú átadás esetén mégis beazonosíthatóvá válhatnak külső, harmadik felek (pl. Facebook, Google) számára. A Bankmonitor érzékeny pénzügyi, banktitoknak minősülő információkat is megtud az ügyfeléről, ezeket azonban a jogszabályi előírásoknak megfelelően banktitokként kezeli. Meglátásom szerint további kockázati tényező az lenne, ha a Bankmonitor által garantált objektivitás megsérülne, hiszen ez a hazai viszonylatban meghatározó platform nagyban tudná befolyásolni az ügyfelek pénzügyi választásait.

6. KÖVETKEZTETÉSEK ÉS JAVASLATOK

A dolgozat egyik célja az volt, hogy esettanulmányokat felhasználva szemléltessem, hogy a digitális pénzügyi szolgáltatók hogyan változtatják meg a fizetési megoldások piacát, valamint mennyire biztosított az új megoldások közötti átjárhatóság. Dolgozatomban többek között azt is vizsgáltam, hogy milyen kockázatokat jelentenek a digitális pénzügyi szolgáltatók a fizetési forgalom biztonságos lebonyolítására, illetve górcső alá vettem a hálózatosodásból eredő kockázatokat is. Az esettanulmányok elkészítése előtt releváns hazai és nemzetközi szakirodalmi forrásokat dolgoztam fel, annak érdekében, hogy bemutassam a legfontosabb diszruptív pénzügyi technológiákat és azok alkalmazásából eredő kockázatokat.

A feldolgozott szakirodalmi források szintetizálása alapján megállapítható, hogy a pénzügyi szolgáltatások nyújtását erőteljesen meghatározza a platformizáció. A hatalmas platformok üzemeltetői közül a BigTech vállalkozások rendelkeznek a legnagyobb piaci erővel. Az elmúlt időszakban egyre többen nyújtanak közülük pénzügyi szolgáltatásokat is. Az ügyfelek platformon rögzített választásainak folyamatos nyomon követése lehetővé teszi számukra a személyre szabott szolgáltatásnyújtást.

Meglátásom szerint a pénzügyi technológiai fejlesztések növelték a szektor hatékonyságát, azonban a FinTech használata számos újszerű kockázatot is felvethet. A pénzügyi szolgáltatási folyamatok során – részben a PSD2 nyílt bankolási szabályai, és az infrastruktúra szolgáltatók miatt – az adatok sok szereplőn futhatnak keresztül, azonban ez a fajta hálózatosodás negatív hatást is kiválthat, hiszen így több fajta támadási felület áll az adathalászok rendelkezésére. Az adatokat érintő kiberkockázat, illetve a csalások típusai két nagy csoportra oszthatók. Az első kategória a személyes hitelesítési adatokkal történő visszaélés, melynek során a csalók a megszerzett adatok segítségével indítanak átutalásokat a saját számlájukra. A második kategória pedig a megtévesztésen alapuló visszaélés, mely esetében pedig a csalók valamilyen hazugság segítségével veszik rá az ügyfelet arra, hogy utaljon át pénzt nekik. Az adathalászok az egyre kifinomultabb módszereinek köszönhetően még a magas biztonságú rendszerekbe is képesek betörni, így a kiberbiztonsági intézkedések folyamatos fejlesztése elengedhetetlen.

Magyarországon az azonnali fizetés bevezetése óta egyre népszerűbbek az elektronikus fizetési módok. Megállapítható, hogy a magas POS terminál díjak miatt az olcsóbb megoldást kínáló, azonnali fizetésre épülő másodlagos azonosítók és QR-kódok alkalmazása a fizetés során kiváló lehetőséget jelent a kereskedők számára. Az új megoldások közötti átjárhatóságot hazai viszonylatban, az azonnali fizetés tekintetében a Magyar Nemzeti Bank által publikált

útmutatók biztosítják, azáltal, hogy egységes technikai háttérrel adnak a különböző fizetési megoldások létrehozásához a szolgáltatók számára.

A vizsgált vállalkozások esettanulmányainak rövid összefoglalását az alábbi táblázat (7. táblázat) tartalmazza. Az esettanulmányokon keresztül jól látható, hogy a szakirodalomban megfogalmazott elméleti koncepciók nagyrésze megvalósul a vizsgált vállalkozások gyakorlatában.

7. táblázat: A vizsgált vállalkozások esettanulmányainak rövid összefoglalása

Szemponatok	Barion Payment Zrt.	FinTechX Technologies Zrt.	SEON Technologies Kft.	Bankmonitor Kft.
Alkalmazott diszruptív technológia, üzleti modell	- e-tárca - külső és belső használatú fizetési kapu - KYC - BigData - AI, gépi tanulás - FinTech-enabled Marketplace - adatmonetizáció	- PFM - AISP - API - felhő - white-label FinTech fejlesztés - license-as-a-service - platform-as-a-service	- BigData - KYC - AI, gépi tanulás - API - adatgazdagítás - magas színvonalú UX, UI - online tranzakció csalás-megelőzés	- BigData - összehasonlító platform szolgáltatás - online kalkulátor - digitális ügynök és közvetítő (E2E)
Kockázati források	- hálózatosodás - érzékeny pénzügyi-, és ügyféladatok kiszivárgása - adatokkal való visszaélés, megtevesztés - AI miatt kontroll elvesztése	- külső fél ékelődik be a folyamatokba - hálózatosodás - érzékeny pénzügyi-, és ügyféladatok kiszivárgása - adatokkal való visszaélés, megtevesztés - adatátadás nem feltétlenül biztonságos szereplőknek	- hálózatosodás - érzékeny pénzügyi-, és ügyféladatok kiszivárgása - adatokkal való visszaélés, megtevesztés - manuális csalás engedélyezés - AI miatt kontroll elvesztése	- szubjektív tanácsadás általi manipuláció - banktitoknak minősülő érzékeny pénzügyi-, és ügyféladatok adatok kiszivárgása

Forrás: Saját szerkesztés

Az esettanulmány során vizsgált FinTech vállalkozások mindegyike diszruptív pénzügyi technológiákkal dolgozik, többen is használnak gépi tanulást és egyéb mesterséges intelligenciára alapuló megoldást. Meglátásom szerint a kritikus döntéshozatal kapcsán alkalmazott AI technológiák a gyorsaságon és hatékonyságon túl felvethetik a kontroll elvesztésének lehetőségét, vagy annak hatékonyságának romlását.

Többen kihasználják a Big Data által kínált előnyöket, hogy a megszerzett adatok megfelelő feldolgozását követően, az eredmények alapján még nagyobb ügyfélélményt nyújtó szolgáltatást tudjanak biztosítani. Az adathalászat a Big Data-val dolgozó pénzügyi szolgáltatókra és azok ügyfeleire is veszélyt jelenthet. Az érzékeny pénzügyi-, és ügyféladatak kiszivárgása az ügyfelek GDPR jogainak megsértése mellett visszaélésre ad lehetőséget a csalók számára. A kiberbűnözés technológiai fejlettsége alkalmanként túllépi a védelmi intézkedések hatékonyságát, így a kiberbiztonsági intézkedések folyamatos fejlesztése elengedhetetlen.

Az infrastruktúra, illetve felhőalapú szolgáltatások, valamint a harmadik feles szolgáltatóként való beékelődés a folyamatokba azt eredményezi, hogy az érzékeny információk több szereplőn futnak keresztül, ami a hálózatosodásból fakadó kockázatokat mutatja. Annak ellenére, hogy az említett vállalkozások mindegyike kiemelt figyelmet fordít a biztonsági megoldásokra, a hackerek általában mindig egy lépéssel előrébb járnak, így fokozott óvatosság szükséges ezekben a kérdésekben.

Meglátásom szerint a FinTech szektorban működő vállalkozások piaci pozíciója szoros összefüggésben van az ügyfélélménnyel, aminek része az árazás. Éppen ezért az ügyfél számára ingyenes szolgáltatásnyújtás – melynek háttérében persze vannak bevételek – rendkívül hatékony módja a nagyszámú fogyasztói réteg megszerzésének, ezáltal egy nagyobb piaci részesedés elérésének. Véleményem szerint a bankok és a FinTech vállalkozások együttműködésének segítése kiemelt fontosságú a hagyományos értékek megőrzése és a diszruptív technológiák terjedésének elősegítése szempontjából. A diszruptív pénzügyi technológiák alapjainak megértése a dolgozók, illetve a vezetőség részéről segít elkerülni az AI alkalmazásából eredő, döntéshozatalhoz kapcsolódó kontroll hatékonyságvesztését.

7. ÖSSZEFOGLALÁS

A pénzügyek egyre inkább összefonódnak a technológiai újításokkal, az elektronikus fizetési lehetőségek használatának terjedése pedig egyre inkább jellemző Magyarországon is. A pénzügyek területét felforgató digitalizáció és a diszruptív technológiák begyűrűzése a pénzügyi szolgáltatásokba átformálta a hagyományos pénzügyi szektort. Felgyorsult az adatfeldolgozás és hatékonyabb lett a szolgáltatásnyújtás. A hatalmas platformüzemeltetők közül leginkább a BigTech cégek emelkednek ki, amelyek IT szolgáltatásaik mellett pénzügyi szolgáltatásokat is elkezdtek nyújtani. Az ügyfelek platformon rögzített választásainak folyamatos nyomon követése pedig lehetővé teszi a személyre szabott szolgáltatásnyújtást, hiszen az ügyféligények felmérése elsődleges forrásból történik. A PSD2 EU-s szabályozás megnyitotta a kapukat a nyílt bankolás felé, így a bankok az ügyfelek előzetes engedélyét követően kötelesek harmadik feles – engedéllyel rendelkező – szolgáltatók számára kiadni az ügyfelek pénzügyi adatait. Az adatok sok szereplőn futhatnak keresztül, gyakran felhőalapú megoldásokat is alkalmaznak a szolgáltatók, ez a fajta hálózatosodás azonban negatív hatással bír, hiszen így nagyobb számú támadási felület áll a hackerek, adathalászok rendelkezésére.

Dolgozatomban a releváns hazai és nemzetközi szakirodalmi források szintetizálásán keresztül mutattam be a legfontosabb diszruptív pénzügyi technológiákat és azok alkalmazásából eredő kockázatokat. Ezt követően négy magyarországi FinTech vállalkozáson keresztül szemléltettem, hogy a vizsgált digitális pénzügyi szolgáltatók hogyan alakítják a hazai pénzügyi megoldások piacát, illetve milyen kockázatot rejt az általuk alkalmazott technológia vagy üzleti modell. Az elektronikus fizetési szolgáltatók közül a Bariont, open banking és adat aggregálás területéről a FintechX-et, online fizetések kockázatelemzői közül a SEON-t, összehasonlító platform üzemeltetők közül pedig a Bankmonitort választottam az esettanulmány vizsgálati alanyai közé. Az esettanulmányokon keresztül jól látható, hogy a szakirodalomban megfogalmazott elméleti koncepciók nagyrésze megvalósul a vizsgált vállalkozások gyakorlatában. Meglátásom szerint a FinTech szektorban működő vállalkozások piaci pozíciója szoros összefüggésben van az ügyfélélménnyel, aminek része az árazás.

Összességében kijelenthető, hogy a pénzügyi technológiai fejlesztések növelték a szektor hatékonyságát, azonban a FinTech használata számos újszerű kockázatot is felvethet. Az infrastruktúra, illetve felhőalapú szolgáltatások, valamint a harmadik feles szolgáltatóként való beékelődés a folyamatokba azt eredményezi, hogy az érzékeny információk több szereplőn futnak keresztül, ami a hálózatosodásból fakadó kockázatokat mutatja. A diszruptív pénzügyi technológiák alapjainak megértése a dolgozók, illetve a vezetőség részéről segít elkerülni az AI

alkalmazásából eredő, döntéshozatalhoz kapcsolódó kontroll hatékonyságvesztését. Megállapítható, hogy a pénzügyi szolgáltatások nyújtását erőteljesen meghatározza a platformizáció. Az ügyfelek platformon rögzített választásainak folyamatos nyomon követése lehetővé teszi számukra a személyre szabott szolgáltatásnyújtást. Az adathalászat a Big Data-val dolgozó pénzügyi szolgáltatókra és azok ügyfeleire is veszélyt jelenthet. Az érzékeny pénzügyi-, és ügyféladatak kiszivárgása az ügyfelek GDPR jogainak megsértése mellett visszaélésre ad lehetőséget a csalók számára. A kiberbűnözés technológiai fejlettsége alkalmanként túllépi a védelmi intézkedések hatékonyságát, így a kiberbiztonsági intézkedések folyamatos fejlesztése elengedhetetlen.

SZAKIRODALMI JEGYZÉK

1. Adevinta Ventures (2021): Fintech-enabled marketplaces – The future of marketplaces part two. <https://static.adevinta.com/wp-content/uploads/2021/09/22092204/Fintech-enabled-Marketplaces-2021-Adevinta-.pdf> (Letöltve: 2021. 09. 30.)
2. AFR (2020): Azonnali fizetés folyamata. afr.hu <https://afr.hu/2020/03/02/azonnali-fizetes-folyamata/> (Letöltve: 2021. 02. 15.)
3. Arner D. – Aurer R. – Frost J. (2020) Stablecoins: risks, potential and regulation. BIS Working Papers No 905. ISSN 1682-7678 (online) <https://www.bis.org/publ/work905.pdf> (Letöltve: 2021. 06. 30.)
4. Azure (2021): Mi az IaaS? – Infrastruktúra-szolgáltatás. azure.microsoft.com. <https://azure.microsoft.com/hu-hu/overview/what-is-iaas/#overview> (Letöltve: 2021. 09. 15.)
5. Feyen E. – Frost J. – Gambocarta L. – Natarajan H. – Saal M. (2021): Fintech and the digital transformation of financial services: implications for market structure and public policy. BIS Papers No 117. ISSN 1682-7651 (online) <https://www.bis.org/publ/bppdf/bispap117.pdf> (Letöltve: 2021. 06. 30.)
6. Deák V. – Kajdi L. – Nemecskó I. (2021): A magyarországi kiskereskedők és vállalatok fizetési szokásainak elemzése. Hitelintézeti Szemle, 20. évf. 2. szám, 2021. június, 33–59. o.
7. Droppa D. – Becsky-Nagy P. (2019): A pénzvilág üdvöskéi: a FinTech-megoldások. In: XIII. Pécsi Pénzügyi Napok – Új kihívások és lehetőségek Konferenciakötet. Pécsi Tudományegyetem Közgazdaságtudományi Kar, Pécs, 20-36.o. (ISBN:978-963-429-456-6)
8. European Banking Authority (2018): EBA report on the impact of fintech on incumbent credit institutions' business models. eba.europa.eu <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2270909/1f27bb57-387e-4978-82f6-ec725b51941/Report%20on%20the%20impact%20of%20Fintech%20on%20incumbent%20credit%20institutions%27%20business%20models.pdf?retry=1> (Letöltve: 2020.08.02.)
9. Financial Stability Board (2019): Decentralised financial technologies – Report on financial stability, regulatory and governance implications <https://www.fsb.org/wp-content/uploads/P060619.pdf> (Letöltve: 2020.08.13.)

10. Flint P. (2021): The Next Frontier for 2-Sided Marketplaces: How Fintech Will Unlock Enormous Value. NFX.com <https://www.nfx.com/post/fintech-enabled-marketplaces/> (Letöltve: 2021. 09. 05.)
11. Industry4 (2021): Big Data. <http://industry4.hu/hu/fogalomtar/big-data> (Letöltve: 2021. 09. 15.)
12. Kajdi L. – Nemecskó I. (2020): A kártyás fizetési mód területi jellemzői Magyarországon. Hitelintézeti Szemle, 19. évf. 1. szám, 2020. március, 65–89. o.
13. Katona T. (2021): Decentralizált pénzügy – A blokkláncon működő pénzlegó-rendszer lehetőségei. Hitelintézeti Szemle, 20. évf. 1. szám, 2021. március, 74–102. o.
14. Kerényi Á. – Molnár J. – Müller J. (2018): Veszedelmes viszonyok a bankok és a fintechek között? Gazdaság és Pénzügy (G.É.P.), 5. évf. 1 sz. 88-99. o.
15. Kerényi Á. – Müller J. (2019): Szép új digitális világ? – A pénzügyi technológia és az információ hatalma. Hitelintézeti Szemle, 18. évf. 1. sz., 5-33. o.
16. KPMG (2021): Pulse of Fintech H2'20. <https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/02/pulse-of-fintech-h2-2020.pdf> (Letöltve: 2021. 03.01.)
17. Magyar Nemzeti Bank (2020): Fizetési Rendszer Jelentés. Magyar Nemzeti Bank, Budapest. ISSN 2498–7077 (on-line) <https://www.mnb.hu/letoltes/fizetesi-rendszer-jelentes-2020.pdf> (Letöltve: 2021. 03. 14.)
18. Magyar Nemzeti Bank (2021a): Fintech és digitalizációs jelentés. Magyar Nemzeti Bank, Budapest. ISSN 2732-3137 (on-line) <https://www.mnb.hu/kiadvanyok/jelentesek/fintech-es-digitalizacios-jelentes/fintech-es-digitalizacios-jelentes-2021-majus> (Letöltve: 2021. 06. 21.)
19. Magyar Nemzeti Bank (2021b): Fizetési Rendszer Jelentés. Magyar Nemzeti Bank, Budapest. ISSN 2498–7077 (on-line) <https://www.mnb.hu/letoltes/fizetesi-rendszer-jelentes-2021.pdf> (Letöltve: 2021. 08. 14.)
20. MasterCard (2021): A fizetési ökoszisztéma védelme. mastercard.hu. <https://www.mastercard.hu/content/mccom/hu-hu/merchants/safety-security/security-recommendations/site-data-protection-PCI.html> (Letöltve: 2021. 08. 02.)
21. Müller J. – Kerényi Á. (2021): Kiútkeresés a digitális pénzügyi innovációk labirintusában – A digitális pénzügyi rendszer szabályozási kihívásainak csapdája. Hitelintézeti Szemle, 20. évf. 1. szám, 2021. március, 103–126. o.

22. Németh M. (2019a): Újabb fontos mérföldkő a nyílt bankolásban: elindult az EU-s központi regiszter. FINTECHZONE.hu <https://fintechzone.hu/ujabb-fontos-merfoldko-a-nyilt-bankolasban-elindult-az-eu-s-kozponti-regiszter/> (Letöltve: 2020. 02. 15.)
23. Németh M. (2019b): 12 nap a PSD2 indulásáig, de nincsenek megfelelő banki API hozzáférések. FINTECHZONE.hu <https://fintechzone.hu/12-nap-a-psd2-indulasaig-de-nincsenek-megfelelo-banki-api-hozzaferesek/> (Letöltve: 2020. 02. 15.)
24. Peters B. (2021): Fintech Cybersecurity Trends in 2021. IT Security Expert Blog https://blog.itsecurityexpert.co.uk/2021/02/fintech-cybersecurity-trends-in-2021.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+securityexpert+%28IT+Security+Expert%29 (Letöltve: 2021.08.18.)
25. Prágay I. (2018): Fizetési forgalom és digitalizáció. Gazdaság és Pénzügy (G.É.P.), 5. évf. 1 sz. 74-87. o.
26. RowanHill Digital (2020): Mennyibe is kerülne? https://rowanhilldigital.com/blog/Mennyibe-is-kerulne?fbclid=IwAR1VYFNyA0EuCaK1SBpx5F2_q6pOauuRVuSnc9V9KYuGfPEir98RuCm76x4 (Letöltve: 2020.10.12.)
27. Schenk T. (2018): Digitális forradalom a bankszektorban. Gazdaság és Pénzügy (G.É.P.), 5. évf. 1 sz. 100-112. o.
28. Schmidt Z. (2018): PCI DSS kereskedőknek: mikor kell tanúsítvány az online fizetéshez? Kosárérték.hu <https://kosarertek.hu/uzemeltetes/pci-dss-kereskedoknek-mikor-kell-tanusitvany-az-online-fizeteshez/> (Letöltve: 2019. 11. 23.)
29. Végső T. – Belházyne Illés Á. – Bódi-Schubert A. (2018): Késspénz vagy kártya? A magyar lakosság fizetési szokásainak feltáró elemzése. Pénzügyi szemle, 63. évf. 4. sz. 455-479. o.
30. Végső T. (2020): A magyarországi késspénzkereslet változásának összehasonlító elemzése. Hitelintézeti Szemle, 19. évf. 1. szám, 2020. március, 90–118. o. DOI: <http://doi.org/10.25201/HSZ.19.1.90118> (Letöltve: 2021.05.02.)

Esettanulmányok során felhasznált források:

- FinTech Group (2020): HUNFINTECH 20/20: A Magyar FinTech Book. FinTech Group. https://FinTechzone.hu/wp-content/uploads/2020/05/HUNFINTECH_2020_MAGYAR_FINTECH_BOOK_e-book_WEB.pdf (Letöltve: 2021. 08. 31.)
- MAFISZ (2021): <https://mafis.hu/> (Letöltve: 2021. 08. 05.)

- T-SYSTEMS Magyarország Zrt. (2016): HUNFINTECH25 https://FinTechzone.hu/wp-content/uploads/2017/03/T_Systems_2016HunFinTech25_kiadvany.pdf (Letöltve: 2021. 02. 10.)
- OPTEN (2021): <https://www.opten.hu/> (Letöltés dátuma: 2021. 05. 01.)

Barion Payment Zrt.:

- Barion Payment Zrt. (2021): A honlapon található adatok és információk. <https://www.barion.com/hu/> (Letöltve: 2021. 09. 01.)
- Boros Norbert (2019): 10 üzleti modell 10 percben. The Innovation Design Blog. <https://innovationdesign.hu/business-design/10-uzleti-modell-10-percben/> (Letöltve: 2021. 08. 29.)
- Kiss S. (2021a): Online mélyinterjú a Barion Payment Zrt. alapító vezérigazgatójával, Kiss Sándorral. Webex meeting, 2021. 10. 18.
- Money.hu (2014): Bíró Tamás: Mi az a Barion és miért járunk jól, ha ezzel fizetünk? BankRáció. <https://www.money.hu/cikk/428-biro-tamas-mi-az-a-barion-es-miert-jarunk-jol-ha-ezzel-fizetunk> (Letöltve: 2021. 08. 20.)
- SalesForm (2021): Barion payment, avagy bankkártyás fizetés. <https://www.rendelesiurlap.hu/cikk/barion-payment-avagy-bankkartyas-fizetes> (Letöltve: 2021. 08. 20.)

FinTechX Technologies Zrt.:

- Aggreg8.io (2021): A honlapon található adatok és információk. <http://aggreg8.io/> (Letöltve: 2021. 07. 02.)
- Andor M. (2016): Mit adnak nekünk a legmenőbb magyar FinTech cégek? – Wyze. FinTechZone.hu <https://FinTechzone.hu/mit-adnak-nekunk-a-legmenobb-magyar-FinTech-cegek-Wyze/?fbclid=IwAR3YAQYV-nVabgouA3nRmJ7R9Q4I5pHIT6hL2PZ3f0hskoLpAgnFs4O-Mtk> (Letöltve: 2021. 08. 01.)
- Andor M. (2017): Fintech ragasztót fejleszt egy magyar startup. FinTechZone.hu <https://FinTechzone.hu/FinTech-ragasztot-fejleszt-egy-magyar-startup/> (Letöltve: 2021. 08. 23.)
- BrandChannel (2018): Tényleg elég egy jó ötlet a sikeres vállalkozáshoz? hvg.hu https://hvg.hu/brandchannel/dekoratio_20181221_Tenyleg_eleg_egy_jo_otlet_a_sikeres_vallalkozashoz (Letöltve: 2021. 06. 22.)

- FinTechX Technologies Zrt. (2021): A honlapon található adatok és információk. <https://FinTechx.digital/> (Letöltve: 2021. 07. 02.)
- Lemák G. (2018): Több ezer FinTech cégből a TOP10-be – Interjú Gémes Tamással, a FintechBlocks társalapítójával. FinTechZone.hu <https://FinTechzone.hu/tobb-ezer-FinTech-cegbol-a-top10-be-interju-gemes-tamassal-a-FinTechblocks-tarsalapitojaval/> (Letöltve: 2021. 08. 22.)
- Turzó Á. P. (2019): Feltűnt négy magyar cég, amely felforgatná, amit a bankolásról eddig gondoltál. Portfólió.hu <https://www.portfolio.hu/bank/20191220/feltunt-negy-magyar-ceg-amely-felforgatna-amit-a-bankolasrol-eddig-gondotal-410197> (Letöltve: 2021. 08. 12.)
- Wzye.me (2021): A honlapon található adatok és információk. <http://Wzye.me/index.html> (Letöltve: 2021. 08. 02.)

SEON Technologies Kft.:

- Digital Natives (2021): UX vs UI – Mi a különbség? digitalnatives.hu <https://www.digitalnatives.hu/hu/ui-ux/> (Letöltve: 2021. 09. 05.)
- FINTECHZONE (2017): Két magyar fintech cég száll harcba a kibercsalók ellen. fintechzone.hu <https://fintechzone.hu/magyar-fintech-startupok-a-csalok-ellen-barion-seon/> (Letöltve: 2021. 08. 02.)
- FINTECHZONE (2021): 10 millió eurót kapott a magyar fintech startup, a SEON. fintechzone.hu <https://fintechzone.hu/10-millio-eurot-kapott-a-magyar-fintech-startup-a-seon/> (Letöltve: 2021. 08. 01.)
- Kiss S. (2021b): Barion – Leading Payment Gateway Saves 50% Work Hours and Keeps Acquiring Costs At Bay. seon.io <https://seon.io/resources/case-study/barion-payment-gateway-saves-work-hours/> Letöltve: 2021. 08. 03.)
- SEON Technologies Kft. (2021): A honlapon található adatok és információk. <https://seon.io/> (Letöltve: 2021. 08. 25.)

Bankmonitor Kft.:

- Bankmonitor Kft. (2021): A honlapon található adatok és információk. <https://bankmonitor.hu/> (Letöltve: 2021. 09. 01.)
- Domokos L. (2021): A Hiventures beszállt a Bankmonitorba. napi.hu <https://www.napi.hu/magyar-vallalatok/hiventures-bankmonitor-befektetes.731518.html> (Letöltve: 2021. 09. 02.)

- FINTECHZONE (2020): Elindult a selfie-fotós számlanyitás a CIB Banknál. Otthonról, videóazonosítás nélkül nyithatunk bankszámlát. [fintechzone.hu
https://fintechzone.hu/elindult-a-selfie-fotos-szamlanyitas-a-cib-banknal-otthonrol-videoazonositas-nelkul-nyithatunk-bankszamlat/](https://fintechzone.hu/elindult-a-selfie-fotos-szamlanyitas-a-cib-banknal-otthonrol-videoazonositas-nelkul-nyithatunk-bankszamlat/) (Letöltve: 2021. 09. 02.)