A-PBT-A-34/2013. Ajánlás

A Pénzügyi Békéltető Testület dr. L.P. ügyvéd által képviselt T.J. (xxx szám alatti lakos, a továbbiakban: Kérelmező) – ABC Bank (yyy, a továbbiakban: pénzügyi szolgáltató) ellen benyújtott kérelmére indult pénzügyi fogyasztói jogvita rendezésére irányuló eljárásban, a 2013. július 10. napján megtartott meghallgatáson az alábbi

AJÁNLÁST

tette:

A Pénzügyi Békéltető Testület ajánlja, hogy a pénzügyi szolgáltató az xxx-én történt károkozás előtti eredeti állapotot állítsa helyre úgy, hogy fizesse meg a Kérelmező részére

- az xxx-én feltört betétjére járó, szerződés szerinti kamatot, valamint az eredeti lejáratot követő naptól a szerződéses kamattal növelt betétösszegre a kifizetés napjáig számított törvényes késedelmi kamatot;
- az általa látra szólóan elhelyezett és xxx-én átutalt összeget, és az utána járó, xxx napjától a kifizetés napjáig számított törvényes késedelmi kamatot.

A Pénzügyi Békéltető Testület ajánlja továbbá, hogy a pénzügyi szolgáltató az xxx-én teljesült vitatott tranzakció során a hitelkeretből felhasznált összeg vonatkozásában a Kérelmezővel szemben semmilyen követelést ne érvényesítsen.

Az ajánlás ellen fellebbezésnek helye nincs, azonban annak kézbesítésétől számított 15 napon belül hatályon kívül helyezése kérhető a Fővárosi Törvényszéktől, ha a tanács összetétele vagy eljárása nem felelt meg a Pénzügyi Szervezetek Állami Felügyeletéről szóló 2010. évi CLVIII. törvény (a továbbiakban: Psztv.) rendelkezéseinek, a Pénzügyi Békéltető Testületnek nem volt hatásköre az eljárásra, a kérelem meghallgatás nélküli elutasításának lett volna helye.

A pénzügyi szolgáltató az ajánlás hatályon kívül helyezését a fentieken túl – az ajánlás részére történt kézbesítésétől számított tizenöt napon belül – akkor is kérheti a Fővárosi Törvényszéktől, ha az ajánlás tartalma nem felel meg a jogszabályoknak.

Ha a pénzügyi szolgáltató az ajánlásnak nem tesz eleget, a Pénzügyi Békéltető Testület – a Kérelmező nevének megjelölése nélkül – jogosult a jogvita tartalmának rövid leírását és az eljárás eredményét legkorábban az ajánlásnak a pénzügyi szolgáltató részére történt kézbesítésétől számított hatvan nap elteltével nyilvánosságra hozni.

A Pénzügyi Békéltető Testület felhívja a pénzügyi szolgáltatót és a Kérelmezőt, hogy jelen ajánlás végrehajtásáról az ajánlás kézhezvételét követő 60 napon belül írásban tájékoztassák a Pénzügyi Békéltető Testületet.
A Pénzügyi Békéltető Testület ajánlása nem érinti a Kérelmezőnek azt a jogát, hogy a pénzügyi szolgáltatóval szembeni igényét bírósági eljárás keretében érvényesítse.

A Pénzügyi Békéltető Testület döntését a Psztv. 94. § b) pontja, 97. §-a, valamint 100. § (1) bekezdése alapján hozta meg.

INDOKOLÁS

A Kérelmező 2013. április 11. napján érkezett kérelmével fordult a Pénzügyi Békéltető Testülethez pénzügyi fogyasztói jogvita rendezése érdekében. Kérelmében előadta, hogy a pénzügyi szolgáltatónál vezetett számlájáról xxx-én „megbízás nélkül" történt 2.148.993,- forint összegű átutalás egy idegen, harmadik pénzügyi szolgáltatónál vezetett számlára. A Kérelmező előadta, hogy tudomása szerint ugyanezen a napon más fogyasztók is hasonló módon károsodtak.

A Kérelmező előadta továbbá, hogy a pénzügyi szolgáltató internetes felületére az xxx-nak, yyy-nak és jelszavának megadásával, majd ezt követően a pénzügyi szolgáltató által SMS-ben küldött jelszó beírásával lehet belépni. A Kérelmező előadta azt is, hogy a belépést követően bármilyen utalás elindítható, az utalást megerősítő jelszót SMS-ben csak az xxx-i események óta küld a pénzügyi szolgáltató, addig csak az az ügyfél kapott ilyen SMS-t, aki azt a szerződés megkötésekor kérte.

A Kérelmező előadta, hogy amikor xxx-én be akart lépni a bank internetes felületére, a fent felsorolt adatok megadását követően a belépéshez szükséges kódot tartalmazó SMS-t megkapta, ezt követően azonban már nem volt lehetősége azt beírni, mert az erre szolgáló felület nem jelent meg (folyamatosan töltődött a honlap), majd az SMS-kód megadására adott idő is letelt.

A Kérelmező előadta azt is, hogy másnap személyesen ment be a bankba, hogy elindítsa a kívánt utalást, de azt a tájékoztatást kapta, hogy nem jó a rendszer, ezért végül készpénzben fizette be a célszámlára az utalni próbált összeget.

A Kérelmező előadta továbbá, hogy csak yyy napján tudta meg, hogy a bankszámlájáról eltűnt a pénze, és ekkor bejelentést tett a pénzügyi szolgáltatónál, valamint feljelentést tett a rendőrségen. A Kérelmező előadta, hogy a büntetőeljárás a kérelem beadásáig nem járt eredménnyel.

A Kérelmező becsatolt egy kinyomtatott, xxx-én 16:38-kor elküldött elektronikus levelet, amelynek tartalma szerint a pénzügyi szolgáltató internetbanki felülete xxx-én egész nap nem működött annak ellenére, hogy a pénzügyi szolgáltató a kijavítást aznap délre ígérte. A Kérelmező álláspontja szerint ez azt bizonyítja, hogy a pénzügyi szolgáltató rendszerét xxx napján hackertámadás érte.

A Kérelmező előadta, hogy a pénzügyi szolgáltató kárt okozott azzal, hogy amikor észlelte, hogy támadás éri az internetes rendszerét, nem tett meg mindent elvárhatót azért, hogy ügyfeleit – így őt – ne érhesse kár. A Kérelmező álláspontja szerint a pénzügyi szolgáltató nem gondoskodott az informatikai rendszerének kockázatokkal arányos védelméről és a rendszert használó személyek egyértelmű azonosításáról. A Kérelmező véleménye szerint ezt

a pénzügyi szolgáltató is belátta, mivel a vitatott eset óta a tranzakciót megerősítő SMS-t is minden ügyfelének megküldi, arról azonban nem tájékoztatta korábban az ügyfeleit, hogy ennek elmaradása milyen kockázatokkal jár.

A Kérelmező álláspontja szerint a pénzügyi szolgáltató megsértette a Polgári Törvénykönyvről szóló 1959. évi IV. törvény (a továbbiakban: Ptk.) 530. §-át, valamint a hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény (a továbbiakban: Hpt.) 13/C. § (1) bekezdését és (5) bekezdésének a) pontját. A Kérelmező előadta, hogy a pénzügyi szolgáltató jogellenes magatartásával felróhatóan kárt okozott neki, ezért a Ptk. 318. § (1) bekezdése és a 339. § (1) bekezdése alapján kártérítéssel tartozik. A kár összege 2.148.993,- forint tőke (ezt utalták el a számlájáról), valamint az a kamat, amelyet azóta a pénzügyi szolgáltató e lekötött összeg után jóváírt volna neki tekintettel arra, hogy az ismeretlen személy a Kérelmező lekötött betétét is feltörte az utalás előtt.

A pénzügyi szolgáltató a válasziratában előadta, hogy a Kérelmező bankszámlájához hhh-tól kapcsolódik internetes szolgáltatás. A szolgáltatás igénybevétele során az ügyfél azonosítása az xxx jegyű xxx, továbbá az yyy és az ügyfél által tetszőlegesen választott, illetve megadott titkos jelszó megadásával történik. A pénzügyi szolgáltató előadta, hogy a Kérelmező esetén kiegészítő biztonsági funkcióként a belépéshez szükséges xxx-szolgáltatás kapcsolódik az internetes csatorna használatához.

A pénzügyi szolgáltató előadta, hogy a Kérelmező xxx-én 13 óra 54 perckor vette igénybe az internetbanki szolgáltatást. A pénzügyi szolgáltató az azonosító adatok megadását követően – a biztonságos belépés érdekében – 36 másodperccel később SMS-üzenetben küldte ki a kódot a Kérelmező által megadott telefonszámra. A pénzügyi szolgáltató előadta továbbá, hogy a Kérelmező – az általa vitatott tranzakció időpontjában – a belépést a megküldött egyedi kódszám megadásával kezdeményezte az internetes felületen. A pénzügyi szolgáltató előadta azt is, hogy a Kérelmező a pénzügyi szolgáltatónál nem tett bejelentést, hogy telefonját eltulajdonították volna, így az SMS-t a pénzügyi szolgáltató kézbesítettnek tekintette.

A pénzügyi szolgáltató előadta, hogy a sikeres bejelentkezést követően került rögzítésre egy 1.051.000,- forint összegű betétfeltörés, melynek teljesítéséről az yyy-szolgáltatás keretében 14 órakor SMS-üzenetben értesítette a Kérelmezőt. E műveleten kívül 2.148.993,- forint értékű átutalási megbízás is rögzítésre került. A pénzügyi szolgáltató utalt arra, hogy mivel a Kérelmező az aktív tranzakciók végrehajtásához nem igényelte az xxx biztonsági funkciót, ezért a pénzügyi szolgáltató a tranzakciókat további megerősítés nélkül, a rögzített adatoknak megfelelően teljesítette.

A pénzügyi szolgáltató a vitatott átutalási művelettel kapcsolatban az alábbi, okiratokkal alátámasztott, részletes tényelőadást tette:

> – A Kérelmező xxx-én 13 óra 54 perc 36 másodperckor kezdeményezte az internetbanki szolgáltatás igénybevételét.

– A pénzügyi szolgáltató a belépéshez szükséges azonosító adatok megadását követően – a biztonságos belépés érdekében – 13 óra 55 perckor SMS-üzenetben az ügyfél által megadott xxx telefonszámra kiküldte a kódot, melynek a pénzügyi szolgáltatótól történő átvételét a mobilszolgáltató vállalat visszaigazolta.

– Az internetes felületen a belépéshez szükséges kód megadása 13 óra 55 perc 24 másodperckor történt meg.

– Ezt követően 13 óra 55 perc 58 másodperckor a szolgáltatást igénybe vevő személy az xxx számú bankszámla forgalmát ellenőrizte a zzz és xxx közötti időszakra vonatkozóan.

– A számlához kapcsolódó lekötött betétek lekérdezésére 13 óra 56 perc 04 másodperckor került sor, majd 13 óra 57 perc 01 másodperckor az 1.051.000,- forint összegű betétet visszavezették. A pénzügyi szolgáltató a betétfeltörésről az yyy-szolgáltatás keretében 14 órakor SMS üzenetben értesítette a Kérelmezőt, melynek a pénzügyi szolgáltatótól történt átvételét a mobilszolgáltató vállalat visszaigazolta.

– A 2.148.993,- forint értékű átutalás rögzítésére 13 óra 59 perc 29 másodperckor került sor, melynek kedvezményezettje az yyy számú, idegen pénzügyi szolgáltatónál vezetett bankszámla volt. A pénzügyi szolgáltató előadta, hogy mivel a Kérelmező az aktív tranzakciók végrehajtásához nem igényelte az xxx biztonsági funkciót, a tranzakciókat további megerősítés nélkül, a rögzített adatoknak megfelelően teljesítette.

A pénzügyi szolgáltató előadta, hogy a Kérelmező yyy-án tett panaszt, melynek során a betétfeltörést nem, kizárólag az átutalás teljesítését vitatta. A pénzügyi szolgáltató megjegyezte, hogy a Kérelmező a Pénzügyi Békéltető Testülethez benyújtott kérelmében sem vitatja a betétfeltörést.

A pénzügyi szolgáltató előadta, hogy a Kérelmezőt xyz-én kelt levelében tájékoztatta arról, hogy álláspontja szerint a kártérítési igényét nem tartja indokoltnak, mivel az átutalás során banki hiba nem történt. A pénzügyi szolgáltató előadta továbbá, hogy a Kérelmező által előadottak alapján megalapozottan feltételezhető, hogy a Kérelmező olyan számítógépről vette igénybe a pénzügyi szolgáltató internetbanki szolgáltatását, melyen a vírusok, kémprogramok elleni védelem nem volt teljes körű, és emiatt egy xxx nevű trójai programmal fertőződhetett meg számítógépe.

A pénzügyi szolgáltató előadta, hogy a Kérelmezővel megkötött szerződés aláírásával a Kérelmező elfogadta az annak elválaszthatatlan részét képező üzletszabályzatban és hirdetményben foglaltakat, amely előírja, hogy a Kérelmező köteles a közzétett biztonsági előírásokat maradéktalanul betartani és elvégezni. A pénzügyi szolgáltató utalt arra, hogy nem határozza meg ügyfelei részére, hogy pontosan milyen eszközökkel, programokkal hajtsa ezt végre, hanem kizárólag javaslatokat, iránymutatást ad a számítógép védelme érdekében.

A pénzügyi szolgáltató hivatkozott a honlapján olvasható, részletes javaslatokat és tanácsokat tartalmazó biztonsági tájékoztatóra. (xxx)

A pénzügyi szolgáltató előadta, hogy az internetes szolgáltatáshoz kapcsolódóan a xxx biztonsági funkció több éve igényelhető a pénzügyi szolgáltatónál, melynek két opciója van, az egyik a bejelentkezéshez, a másik a tranzakciók végrehajtásához igényelhető. A pénzügyi szolgáltató előadta továbbá, hogy a Kérelmező a pénzügyi szolgáltató internetes szolgáltatásához kizárólag a belépéshez szükséges xxx opciót választotta. A pénzügyi szolgáltató utalt arra, hogy a Kérelmezőnek lehetősége lett volna a tranzakciók végrehajtásához is igényelni ezt a biztonsági beállítást, amely egyébként semmilyen többletköltséget nem jelentett volna számára.

A pénzügyi szolgáltató álláspontja szerint bármely típusú xxx beállítása biztosítja ügyfeleinek a védelmét, ha a megfelelő számítástechnikai védelmet is alkalmazzák. Mivel ezek az eszközök kizárólag az ügyfeleik által ellenőrzöttek, a pénzügyi szolgáltató ezeket nem tudja védeni, felügyelni. Ezért szükséges egy addicionális elem bevezetése, ahol az ügyfelek dönthetik el, hogy saját egyéb védelmi eszközt (vírusirtó, tűzfal stb.), illetve számlahasználati szokásaikhoz igazodva milyen beállítást választanak.

A pénzügyi szolgáltató előadta, hogy az internetbanki felületén xxx-én xxx óra xxx perctől kezdődően figyelemfelhívó üzenetben tájékoztatta ügyfeleit, hogy új internetes támadási módszer terjed hazánkban. A pénzügyi szolgáltató utalt arra, hogy ügyfelei nem csupán a pénzügyi szolgáltató honlapjáról, hanem a Bankszövetség közleményéből és a sajtóban megjelentekből is értesülhettek az ügyfelek számítógépei elleni támadásról és az internetes szolgáltatás biztonságos használatához elengedhetetlen számítástechnikai védelemről.

A pénzügyi szolgáltató utalt arra, hogy annak érdekében, hogy a Kérelmezőéhez hasonló eset előfordulási esélyét csökkentse, a szükséges fejlesztések végrehajtása után yxz-től, az ügyfelei részére addig is rendelkezésükre álló lehetőséget, a tranzakciónkénti xxx-t kötelezővé tette.

A pénzügyi szolgáltató benyújtotta azt a rendszeréből kinyomtatott iratot, amely alapján megállapítható volt, hogy a vitatott internetbank-használat során nem változott az az IP-cím, amelyről a pénzügyi szolgáltató internetbank rendszerébe beléptek, illetve a tranzakciót végrehajtották. A pénzügyi szolgáltató arról nyilatkozott továbbá, hogy informatikai rendszerét nem érte támadás, az minden szempontból sértetlen, erre vonatkozóan egyik bizonyítéka, hogy internetes rendszerét számos ügyfele minden probléma nélkül, elégedetten használta a Kérelmező által vitatott tranzakció napján is.

A pénzügyi szolgáltató válasziratában nem tett alávetési nyilatkozatot és egyezségi ajánlatot.

A Pénzügyi Békéltető Testület eljáró tanácsa 2013. május 27-én, 2013. június 12-én és 2013. július 10-én meghallgatást tartott. A felek mindhárom meghallgatáson megjelentek.

Az első meghallgatáson a felek az általuk előadottakat fenntartották. A Kérelmező előadta, hogy xxx-én volt, amikor a vitatott tranzakcióra sor került. A Kérelmező egyezségi ajánlatot

tett, mely szerint az általa követelt teljes összeg helyett xxx forint megfizetését is elfogadja a vitás ügy lezárása érdekében. A tényállás tisztázása érdekében az eljáró tanács felhívta a pénzügyi szolgáltatót arra, hogy nyilatkozzon arról, hogy a vitatott internetes belépés, illetve átutalás idejében az internetbankos hozzáférés biztonsága érdekében milyen intézkedéseket tettek, milyen módon védték rendszerüket az illetéktelen behatolással szemben (tűzfal, IP-címekről vezetett feketelista stb.). A pénzügyi szolgáltató időt kért az egyezségi ajánlat megfontolására, illetve az eljáró tanács által feltett kérdések megválaszolására.

A meghallgatási időközben a pénzügyi szolgáltató az eljáró tanács felhívására arról nyilatkozott, hogy informatikai rendszerét nem érte támadás, az a vitatott tranzakció időpontjában is minden szempontból sértetlen volt. A pénzügyi szolgáltató előadta, hogy rendszereiket folyamatosan védik behatolásvédelmi- és vírusvédelmi rendszerekkel, valamint tűzfalakkal, melyek közül egyik biztonsági elem sem észlelt sikeres támadást. A pénzügyi szolgáltató álláspontja szerint ebből, illetve a Kérelmező által előadottak alapján megalapozottan feltételezhető, hogy a Kérelmező olyan számítástechnikai eszközről vette igénybe a pénzügyi szolgáltató internetes szolgáltatását, amelyen a vírusok és kémprogramok elleni védelem nem volt teljes körű. A pénzügyi szolgáltató álláspontja szerint a Kérelmező által használt számítógép egy xxx nevű trójai programmal fertőződhetett meg, melynek következtében lehetővé vált az ügyfél által vitatott banki művelet végrehajtása.

A pénzügyi szolgáltató előadta továbbá, hogy a bankok között nincs kötelező jellegű IP-címmegosztási feladat, esetlegesen lehet IP-címátadás, azonban erre a bankok nem alapozhatják a rendszereik védelmét. A pénzügyi szolgáltató álláspontja szerint az IP-cím személyes adatnak minősül, amennyiben az az ügyfélre visszakövetkeztethető, ezért az érintett ügyfél tudomása nélkül annak átadása más bank felé illegális tevékenység is lehet. A pénzügyi szolgáltató előadta, hogy a jogszabályi előírások maximális figyelembevételével a saját érdekkörében alkalmazhat esetlegesen IP-címekkel kapcsolatos riasztást (feketelistás IP-cím), azonban előírás, kötelezettség a pénzügyi szolgáltatók számára nincs erre vonatkozóan. A pénzügyi szolgáltató utalt arra, hogy jelen vitás ügyben arról az IP-címről, amelyről a belépés történt, nem volt semmilyen információja, amely feketelistára vételt vagy riasztást indokolt volna, egyébként pedig a pénzügyi szolgáltató ügyfelei a pénzügyi szolgáltató internetbanki szolgáltatását bárhonnan igénybe vehetik.

A pénzügyi szolgáltató korábbi álláspontját fenntartotta, mely szerint az átutalás teljesítése során banki hiba nem történt, és a Kérelmező egyezségi ajánlatát – azaz, hogy a Kérelmező követeléséből enged, így a 2.148.993,- forint helyett xxx forintra tart igényt – a pénzügyi szolgáltató nem fogadta el.

A második meghallgatáson a felek fenntartották az addig előadottakat. A további kérdések tisztázása, illetve a tényállás pontos megállapítása érdekében az eljáró tanács a pénzügyi szolgáltatót felhívta, hogy a harmadik meghallgatást megelőzően írásban (a továbbiakban: második kiegészítő válaszirat) nyilatkozzon arról, hogy

1. a zxy-ban köztudottan számos esetben bekövetkezett internetes visszaélésekről, illetve csalásokról (melynek következtében ismeretlen elkövetők elutalták a bankszámlán lévő pénzt) hogyan és mikor szerzett tudomást,

2. a zxy-ban történt internetbanki visszaélésekkel kapcsolatban hány panaszbejelentés érkezett a pénzügyi szolgáltatóhoz, ezeket hogyan kezelte,

3. a zyx-ban történt internetbanki visszaélésekkel kapcsolatban hogyan tájékozódott, milyen adatokat gyűjtött az ügyfeleinek gépét támadó vírusról, ennek keretében – ügyfeleinek tájékoztatásán túl – milyen biztonsági lépéseket tett annak érdekében, hogy ügyfeleit ne tévessze meg az internetbank honlapját lemásoló vírus,

4. a zyx-ban történt internetbanki visszaélésekkel kapcsolatban folytatott-e le belső informatikai ellenőrzést, illetve vizsgálatot, ha igen, milyen megállapítások, illetve cselekvési terv született, az erre vonatkozó okiratokat (jegyzőkönyvek, döntések, cselekvési, illetve megvalósítási tervek stb.) csatolja be,

5. a zyx-ban történt internetbanki visszaélésekkel kapcsolatban folytatott-e le belső ellenőrzést, ha igen, az ezzel kapcsolatosan keletkezett okiratokat (jegyzőkönyvek, belső ellenőr megállapításai stb.) csatolja be.

Az 1. pont vonatkozásában a pénzügyi szolgáltató azt nyilatkozta, hogy az ügyfelek sérelmére elkövetett internetes csalás gyanúja miatt aaa-án yyy óra yyy perckor érkezett az első ügyfélbejelentés, melyet telefonos ügyintézőjük rögzített.

A 2. pont vonatkozásában a pénzügyi szolgáltató közölte az ügyfelek sérelmére zxy hónapban elkövetett internetes visszaélésekkel kapcsolatban érkezett panaszbejelentések számát. A pénzügyi szolgáltató előadta, hogy minden bejelentést egyedi esetként kezelt, és a törvényes válaszadási határidő betartásának figyelembevételével teljes körűen tájékoztatta az ügyfeleit. A pénzügyi szolgáltató közölte továbbá a vitatott tranzakció időszakában (xxx, xxx óra xxx perc és zzz óra xxx perc között) regisztrált sikeres bejelentkezések nagy számát, és arra hivatkozott, hogy ebben az időszakban vitatott átutalás kizárólag a Kérelmező esetében teljesült. A pénzügyi szolgáltató álláspontja szerint ez is a banki rendszer sértetlenségét támasztja alá.

A 3. ponttal kapcsolatban a pénzügyi szolgáltató kifejtette a következőket. Az aaa esetek hátterében az xxx néven ismert károkozó volt, amellyel kapcsolatban kijelenthető, hogy az nem másolja le a pénzügyi szolgáltató honlapját. A pénzügyi szolgáltató előadta, hogy sem az eset időpontjában, sem az azóta eltelt időszakban nem kapott olyan bejelentést, amely azt erősítené, hogy a pénzügyi szolgáltató honlapját valaki lemásolta volna. A pénzügyi szolgáltató előadta azt is, hogy önmagában a honlap lemásolása nem okozhat kárt, hiszen az ügyfele által megadott telefonszámra SMS-ben kiküldött egyedi kód megadása nélkül be sem lehet lépni az internetbankba, így tranzakciókat sem lehet indítani. A pénzügyi szolgáltató előadta továbbá, hogy fontos tény az, hogy az xxx alkalmazás nem a pénzügyi szolgáltató szervereit, hanem az ügyfelek hálózatra kötött eszközeit támadja (támadta) meg oly módon,

hogy feltelepül a felhasználó hálózatra csatlakoztatott eszközére (az esetek jelentős többségében a felhasználó „közreműködésével”) és a böngészőbe, a számítástechnikai eszköz memóriájában lévő adatokat írja át, információkat tüntet el, a felhasználó tevékenységeit (böngészőadatokat, beviteli mezőben megadott vagy csatolt adatokat, billentyűleütést stb.) továbbítja a támadók felé. Ezzel „hátsó kaput” nyit a támadóknak, hogy azok szabadon hozzáférhessenek az adott eszközhöz, blokkolja a vírusvédelmi szoftvert, valamint elérhetetlenné teszi azok frissülését stb.

A pénzügyi szolgáltató előadta, hogy az xxx sikeres feltelepülése – ügyféloldali és nem banki rendszert érintő – több hiányosság esetén is bekövetkezhet, ilyen lehet a vírusvédelem hiánya, vagy nem naprakész vírusvédelmi adatbázis, az operációs rendszer frissítéseinek hiánya, az adott eszközön lévő alkalmazások biztonsági frissítéseinek hiánya, az adminisztrátori jogú felhasználóval végzett böngészés, levelezés, internetről vagy más eszközökről származó fájlok megnyitása stb.

A pénzügyi szolgáltató ismertette, milyen behatolásérzékelő és tűzfalrendszerrel rendelkezik, melyek álláspontja szerint a kor legmagasabb szintű biztonsági elvárásainak megfelelő eszközök. A pénzügyi szolgáltató előadta, hogy az eszközöket és az azokban beállított szabályrendszereket, szűrési feltételeket az üzemeltető munkatársai folyamatosan paraméterezik, a naplóállományokat folyamatosan figyelik, de a rendszerek automatikus riasztást is generálnak. Mindezeken túl az adathálózati forgalomirányító eszközökben is vannak szűrési, hozzáférés-védelmi paraméterek.

A pénzügyi szolgáltató újból előadta, hogy a vitás ügyben érintett időszakban semmiféle eredményes behatolásra utaló nyomot nem észlelt, érzékelt a rendszereiben.

A pénzügyi szolgáltató előadta azt is, hogy mindezeken túl rendszeres időközönként biztonsági teszteléseket hajt végre, a „strómanokat”, gyanús számlaszámokat kiszűri, illetve – ahogyan azt korábban is előadta – yxz-től a tranzakciónkénti xxx-t kötelezővé tette.

A pénzügyi szolgáltató előadta, hogy amint tudomást szerzett arról, hogy ügyfeleinél probléma adódott az internetbanki átutalás közben, felvette a kapcsolatot az elsőként érintett ügyfelek közül néhánnyal, és akik ahhoz hozzájárultak, azoknak a gépeit a helyszínen banki szakemberek átvizsgálták. A pénzügyi szolgáltató előadta továbbá, hogy amint egyértelművé vált számára, hogy minden vizsgált eset mögött az xxx kártevő áll, újabb helyszíni vizsgálatokra nem került sor. A pénzügyi szolgáltató minden esetben feljelentést tett (bár erre semmiféle törvényi kötelezettsége nincs), és kérte ügyfeleit, hogy hasonlóképpen jelezzék az ismeretlen tettes általi károkozást a rendőrség felé.

A 4. és 5. kérdésre a pénzügyi szolgáltató egyben adta meg a válaszát, mely szerint a pénzügyi szolgáltató internet irányába kiajánlott szerverei és alkalmazásai is rendszeres időközönként biztonsági vizsgálatnak vannak alávetve. A pénzügyi szolgáltató internetes informatikai rendszerei folyamatos felügyelet alatt vannak, és a védelmi eszközökön az érintett időszakban sem észlelt eredményes támadást. Ha lett volna bármilyen banki belső rendellenességre gyanút adó esemény, akkor azt a pénzügyi szolgáltató xxx terve alapján

vizsgálta volna, ilyenre okot adó eseményt azonban nem észlelt, a bank rendszereibe nem történt behatolás. A pénzügyi szolgáltató ismételten hangsúlyozta, hogy az xxx kártékony alkalmazás nem a pénzügyi szolgáltató szervereit támadja, hanem az ügyfelek hálózatra kötött eszközeit.

A pénzügyi szolgáltató a korábban tett, IP-címekkel kapcsolatos feketelistáról szóló előadását kiegészítette az alábbiakkal:

A pénzügyi szolgáltató nem vezet feketelistát az IP-címekről, mivel ennek felépítése, karbantartása technikai okok miatt operatívan nem megoldható, és nincs is gyakorlati haszna sem a következők miatt. Az elektronikus banki szolgáltatások előnye, hogy a szerződést kötő ügyfél a világ bármely pontjáról, a nap 24 órájában igénybe veheti azt. Ezen szolgáltatást díjfizetés ellenében veszi igénybe az ügyfél. A pénzügyi szolgáltatónak nem feladata, hogy kövesse az ügyfelek tartózkodási szokásait. A pénzügyi szolgáltató nem tudja eldönteni, hogy melyik számlatulajdonos veszi igénybe a szolgáltatást csak Magyarországról, és ki az, aki rendszeresen utazik, és külföldön is használni szeretné a szolgáltatást. De az IP-cím szűrése még Magyarországon belül sem lehet hatékony, mert az ügyfél Magyarországon is folyamatosan változtathatja a helyét, ami miatt az IP-címe is változik. A pénzügyi szolgáltató ilyen szűrésre nem is ajánl szolgáltatást, mivel a legnagyobb gondosság mellett sem tudná eldönteni az ügyfél IP-címe alapján a tranzakció jogosságát.

A pénzügyi szolgáltató előadta, hogy az internetszolgáltatók jelentős része IP-cím tartományokkal dolgozik, amelyen belül dinamikus címkiosztás történik (DHCP), így az egyes hálózatra kötött eszközök IP-címe akár naponta változhat. Ha egy IP-t feketelistára tesznek, azt az IP-t lehet, hogy másnap már egy nem rosszindulatú eszköz kapja meg kizárva így őt a szolgáltatás eléréséből, ugyanakkor a rosszindulatú eszköz pedig újra lekerül a feketelistáról, mert másik IP-t kapott.

A pénzügyi szolgáltató előadta továbbá, hogy sok internetszolgáltató proxy mögé teszi saját hálózatának a forgalmát (hálózatra kötött eszközöknek kiosztott privát IP-k, néha a szolgáltatási területen kívüli országban van a proxy), így minden, a szolgáltatótól érkező és bemenő forgalom egy (hálózat nagyságától függően néhány) publikus IP címen látszik a publikus hálózat felől. Így a bank oldaláról nem mondható meg, hogy melyik volt a konkrét támadó IP-cím (kedvező esetben a szolgáltató tudja megmondani a saját naplóállományai alapján, ha tárolja ezeket), a forgalomban csak a proxy IP-címe látszik, és annak feketelistára tételével – adott szolgáltató hálózati kialakításától függően – akár több ezer vagy több százezer ügyfél vagy potenciális ügyfél zárható ki a szolgáltatásból.

A pénzügyi szolgáltató előadta, hogy a támadók a saját forgalmukat általában proxyk mögé rejtik, sokszor több proxy-t is használnak egymás után fűzve a támadás kivitelezése során, és ezeket gyakran cserélik is. Mivel minden hálózatra kötött eszköz potenciális proxy is lehet, nem tudhatjuk, hogy melyek a fertőzött, de eddig még rosszindulatú tevékenységre nem használt hálózaton lévő eszközök, így ez alapján az egész publikus IP-tartományt ki lehetne szűrni.

A pénzügyi szolgáltató álláspontja szerint a pénzügyi szolgáltató nem tudja, és éppen ezért nem is vállalhatja fel, hogy minden ügyfelének az IP-címét ellenőrzi a bejelentkezéskor. Az internetbankolás alaplogikája és értelme, hogy megfelelő számítástechnikai eszközön bárhol és bárhonnan lehet használni. Ezen túlmenően az IP-címek feketelistájánál részletezett technikai okok miatt nem létezik olyan eljárás, amellyel teljes bizonyossággal kiszűrhető a bejelentkező IP-cím „tisztasága" vagy „rosszindulatú" volta.

A pénzügyi szolgáltató előadta, hogy az xxx-t bbb-ben vezette be, ekkorra jelentős volt az ügyfélvisszajelzések száma, ami az új biztonsági belépéssel kapcsolatos kényelmetlenségeket taglalta, és sok esetben emiatt felmerült a bankváltás is az ügyfelek részéről. Éppen ezért a bank nagyon körültekintően, csak fokozatosan (az ügyfelek visszajelzései és előzetes reakcióik felmérései alapján) szigorította a belépés folyamatát, így például ccc-től az új szerződéseknél már kötelezővé tette a bejelentkezéses xxx használatát, majd yxz-től a tranzakciós xxx-t (mely változásra már a ddd-én kiküldött postaláda üzenetben felhívta ügyfeleinek a figyelmét). A pénzügyi szolgáltató előadta, hogy a szolgáltatás kötelezővé tétele során figyelemmel kellett lennie arra a tényre is, hogy az elektronikus szolgáltatások igénybevétele szempontjából a ggg egy kiemelt időszak, ekkor az ügyfelek által végzett tranzakciók száma jelentősen emelkedik, így a tranzakciós xxx kötelezővé tétele számos negatív ügyfélvisszajelzést eredményezhetett volna. A pénzügyi szolgáltató álláspontja szerint mindezek egyértelműen alátámasztják, hogy ő az elmúlt évek során több szempontot és körülményt mérlegelve döntött az xxx biztonsági funkció fokozatos szigorításáról. A pénzügyi szolgáltató előadta azt is, hogy azoknak az ügyfeleinek, akik egyáltalán nem rendelkeztek xxx biztonsági funkcióval, eee-én postaláda üzenetben személyre szabottan, a szolgáltatás aktuális beállításához igazodva küldött tájékoztatást a módosításról.

A pénzügyi szolgáltató előadta, hogy igyekezett minden szükséges információt biztosítani az ügyfeleinek, ennek keretében a honlapján külön oldalt készített az internetbank biztonsági tudnivalóiról meghivatkozva a Pénzügyi Szervezetek Állami Felügyeletének ajánlásait is annak érdekében, hogy az ügyfelei akaratuk szerint ők állíthassák be maguknak az általuk biztonságosnak, kényelmesnek és elégségesnek tartott biztonsági opciókat. A pénzügyi szolgáltató utalt arra, hogy mivel az aktívan internetbankoló ügyfelei jelentős többsége ragaszkodik az internet által adott „szabadsághoz" és saját döntéshozatali lehetőségeikhez, ezért az ő elégedettségük érdekében a pénzügyi szolgáltatónak az volt a kiemelt célja, hogy ezt megfelelő keretek között biztosítsa. Ezért csak a fokozatosság elve, egy meghatározott hosszú távú forgatókönyv szerinti szigorítás lehetett a pénzügyi szolgáltató számára a célravezető, melyben a tranzakciós xxx kötelezővé tétele yxz-re lett dátumozva. A pénzügyi szolgáltató megjegyezte, hogy a fokozatosság, az aprólékos előkészítés és tájékoztatás ellenére minden szigorításnál jelentős számú negatív ügyfélreakciót kapott, hiszen a változtatások az ügyfeleknek elsősorban a kényelmetlenebb használhatóságot jelentette: további adat beírása, lassabb bejelentkezési folyamat. A pénzügyi szolgáltató álláspontja szerint az általa végrehajtott hosszú távú yyy terv összhangban volt a biztonsági elvárásokkal és ügyfelei igényeivel, így a módosításokat szinte zökkenőmentesen sikerült elfogadtatnia velük.

A pénzügyi szolgáltató álláspontja szerint az alábbi informatikai szakkérdések merültek fel:

1. A Kérelmező a számítógépét ért támadást megfelelő gondossággal eljárva elháríthatta volna-e?
2. A pénzügyi szolgáltató informatikai rendszerét érte-e támadás? Ha igen, azt megfelelő gondossággal eljárva elháríthatta volna-e?
3. Lett volna-e az informatika jelenlegi fejlettsége, az internet adott működése és az adott ügy körülményei (xxx hiánya a Kérelmező által indított tranzakcióknál) mellett lehetőség arra, hogy a pénzügyi szolgáltató – megfelelő gondossággal eljárva – az átutalási megbízást kiszűrje, annak teljesítését megtagadja?

A pénzügyi szolgáltató előadta, hogy a második kiegészítő válasziratban előadottak nagyrészt a pénzügyi szolgáltató informatikai és bankbiztonsági szakemberei által adott információkon alapulnak. A pénzügyi szolgáltató álláspontja szerint az általa megadott válaszok önmagukban is mind szakmailag, mind logikailag teljes mértékben alátámasztottak, és ismertetik a releváns tényeket is, ugyanakkor e kérdések szakmai alapon történő érdemi felül bírálata, illetve cáfolata csakis szakértő útján történhetne, amelynek kirendelésére azonban a Pénzügyi Békéltető Testület előtti eljárásban nincs lehetőség. A pénzügyi szolgáltató előadta továbbá, hogy mivel álláspontja szerint a Kérelmezőnek további kérdésekre kell válaszolnia, közvetlenül megkereste a Kérelmezőt. A pénzügyi szolgáltató csatolta a Kérelmezőnek közvetlenül írt levelet.

A pénzügyi szolgáltató előadta, hogy álláspontját továbbra is fenntartja, mely szerint az átutalás teljesítése során banki hiba nem történt, emiatt a Kérelmező egyezségi ajánlatát továbbra sem fogadja el.

A harmadik meghallgatáson a felek érdemben fenntartották a korábban előadottakat, továbbá a Kérelmező megválaszolta a pénzügyi szolgáltató által írásban feltett kérdéseket az alábbiak szerint:

1. Pénzügyi szolgáltató: Az xxx-i internetbankoláshoz igénybe vett számítástechnikai eszközön a vitatott tranzakció időpontja és a Testület által megtartott harmadik meghallgatás közötti időszakban történt-e új operációsrendszer-telepítés, melyet megelőzött a merevlemez formattálása?
   Kérelmező: Igen, azóta volt újratelepítés.

2. Pénzügyi szolgáltató: A fent jelzett időszakban történt-e xxx újratelepítés az érintett számítástechnikai eszközön?
   Kérelmező: Igen.

3. Pénzügyi szolgáltató: Milyen operációs rendszert (operációs rendszer típusa, verzió-, servicepack száma) használt a vitatott tranzakció időpontjában azon a számítógépen, amelyről a pénzügyi szolgáltató internetbanki szolgáltatását igénybe vette?
   Kérelmező: xxx-es operációs rendszert.

4. Pénzügyi szolgáltató: Milyen szoftvereket használt a számítógépen (használt szoftverek listája, verziója), amelyről a pénzügyi szolgáltató internetbanki szolgáltatását igénybe vette?
   Kérelmező: xxx volt a böngésző.

5. Pénzügyi szolgáltató: Milyen az internet csatlakozás típusa [ADSL/Kábelnet/mobilnet/wifi (használt hálózati titkosítás fajtája)]?
   Kérelmező: xxx-csatlakozás van.

6. Pénzügyi szolgáltató: A vitatott tranzakció időpontjában milyen védelem alatt állt a rendszer az illetéktelen behatolásokkal szemben?
7. Pénzügyi szolgáltató: Pontosan milyen eszközöket alkalmaztak az érintett számítógép védelmére?
   Kérelmező a 6-7. kérdésre együttesen: Tűzfal a routeren, tűzfal a gépen és xxx vírusirtó.

8. Pénzügyi szolgáltató: Hogyan győződött meg a védelmek megfelelő működéséről?
   Kérelmező: Nem merült fel addig semmilyen gyanús körülmény.

9. Pénzügyi szolgáltató: Milyen módon tudja bizonyítani, hogy a vitatott tranzakció időpontjában a pénzügyi szolgáltató internetbanki szolgáltatásának igénybevételéhez használt számítógép nem volt kártékony alkalmazás (vírus, trójai program stb.) által kompromittálva?
10. Pénzügyi szolgáltató: Miképpen tudja bizonyítani, hogy a vitatott tranzakció időpontjában megfelelően működött a számítógép, melyről a pénzügyi szolgáltató internetbankos szolgáltatásának igénybevételét kezdeményezte?
    Kérelmező a 9-10. kérdésre együttesen: Ezt sehogyan, ezt nem lehet bizonyítani. Ilyet álláspontom szerint senki sem tud bizonyítani. A vírusvédelemről egy felugró ablak tájékoztatott.

11. Pénzügyi szolgáltató: Ki fér az érintett géphez? Van a Kérelmezőn kívül más is, aki jogosultsággal rendelkezik a számítógépen (pl. rendszergazda)?
    Kérelmező: A Kérelmező és a rendszergazda.

12. Pénzügyi szolgáltató: A kérdéses időszakban milyen jogosultsággal használta az operációs rendszert (felhasználó/adminisztrátor)?
    Kérelmező: Az újratelepítés miatt nem tudjuk biztosan, de valószínűleg felhasználó.

13. Pénzügyi szolgáltató: Elolvasta-e a vitatott tranzakciót megelőzően a pénzügyi szolgáltató honlapján található biztonsági tájékoztatást?
    Kérelmező: A tájékoztatást a Kérelmező elolvasta.

A pénzügyi szolgáltató indítványozta továbbá, hogy a Kérelmező kérje ki mobilszolgáltatótól és mutassa be a Pénzügyi Békéltető Testületnek, hogy az xxx telefonszámról milyen SMS-t kapott fff-én és xxx-én.

A pénzügyi szolgáltató a harmadik meghallgatáson úgy nyilatkozott, hogy „aaa-án érkezett hozzánk az első panasz, ekkor elkezdtük vizsgálni saját rendszereinket, mi akkor megvizsgáltuk a bejelentést tevő gépét, és ezen találták meg szakértőink a vírust”.

A kérelem megalapozott.

A felek által tett előadások és a rendelkezésre bocsátott bizonyítékok alapján a Pénzügyi Békéltető Testület eljáró tanácsa az alábbiakat állapította meg.

Az eljáró tanács elfogadta a tényállás megállapításának alapjául a pénzügyi szolgáltatónak a xxx-én 13 óra 54 perc 36 másodperc és 13 óra 59 perc 29 másodperc közötti, internetbanki használatra vonatkozó előadását. A pénzügyi szolgáltató erre a folyamatra vonatkozóan saját rendszeréből nyomtatott okiratot is csatolt, ennek tartalmát az eljáró tanács nem találta aggályosnak. Az eljáró tanács nem fogadta el a Kérelmezőnek azt az állítását, mely szerint a belépéshez szükséges SMS-kódot nem tudta beírni a pénzügyi szolgáltató internetes felületén tekintettel arra, hogy a belépéshez ez mindenképpen szükséges.

Egyebekben a felek között nem is volt vita abban a tekintetben, hogy a pénzügyi szolgáltató internetbanki felületén beléptek, ott betétet törtek fel, továbbá onnan pénz átutalása történt meg. A pénzügyi szolgáltató hivatkozott ugyan arra, hogy a Kérelmező nem panaszolta a betét feltörését, ugyanakkor az eljáró tanács álláspontja szerint a betét feltörése szükségszerű volt ahhoz, hogy a vitatott tranzakcióra sor kerüljön.

Az eljáró tanács álláspontja szerint a felek közötti jogvita lényege az, hogy míg a Kérelmező szerint a pénzügyi szolgáltatónak felróható az, hogy a pénzét illetéktelenek elvihették, addig a pénzügyi szolgáltató álláspontja az, hogy a maga részéről mindent megtett annak érdekében, hogy ügyfeleinek pénzét az internetes támadásokkal szemben is megvédje tekintettel arra, hogy saját informatikai rendszerét megfelelően alakította ki, illetve védi, továbbá ügyfelei számára is kellő tájékoztatást ad az internetbankolás veszélyeiről. A pénzügyi szolgáltató mindezek alapján arra hivatkozott, hogy neki nem felróható az, hogy a Kérelmező számítógépe vírusos volt, így azon keresztül az internetbanki hozzáférésével vissza tudtak élni.

Az eljáró tanács a pénzügyi szolgáltató által az xxx vírusra tett tényelőadás és a becsatolt iratok, illetve a nyilvánosan hozzáférhető információk alapján megállapította, hogy ennek a vírusnak az a lényege, hogy interneten keresztül a felhasználók számítógépére feltelepül – akár úgy is, hogy a felhasználók a tőlük elvárható legmagasabb fokú gondosságot tanúsítják a számítógépük védelme, illetve használata során –, majd amikor a felhasználó az internetbank rendszerébe be kíván lépni, akkor a vírus valamilyen módon megtéveszti a felhasználót, és a továbbiakban az internetbanki hozzáférést más, illetéktelen személy számára biztosítja. Az eljáró tanács megállapította továbbá, hogy az xxx vírus a pénzügyi szolgáltató honlapjának megjelenését módosíthatta, mely nem a honlap forráskódjának fizikai megváltoztatását jelentette, hanem a vírus a honlap bizonyos részeit kitakarta úgy, hogy még az elvárható legmagasabb fokú gondosság mellett sem vehető észre a változtatás. A vírus további

tulajdonsága, hogy a belépési folyamatban olyan képernyőt jeleníthet meg, amelyen hibaüzenet olvasható, ez pedig a felhasználó számára nem feltétlenül felismerhető, hogy valóban a pénzügyi szolgáltató rendszerének hibaüzenetét látja-e vagy sem. Az eljáró tanács álláspontja szerint a pénzügyi szolgáltató informatikai rendszere elleni támadásként értelmezhető az is, ha a támadást nem közvetlenül a pénzügyi szolgáltató szerverei ellen intézik, hanem a honlap megjelenését – akár az ügyfél gépén – módosítják abból a célból, hogy a felhasználókat – azaz pénzügyi szolgáltató ügyfeleit – megtévesszék.

Az eljáró tanács álláspontja szerint egy igazságügyi szakértői vizsgálat sem állapíthatná meg, hogy a vitatott tranzakció napján, illetve időpontjában a Kérelmező számítógépe milyen állapotban volt. Nem lehet utólag – legalábbis ennyi idő elteltével – megállapítani, hogy a Kérelmező gépén milyen vírusvédelmi, illetve egyéb, kártékony programok kiszűrésére alkalmas programok, továbbá böngészők voltak telepítve, ezeknek mi volt a verziója, illetve a vírusirtó programok definíciós adatbázisa mikori frissítésű volt. Az eljáró tanács utal arra, hogy egy naponta használt számítógépen napról napra, sőt óráról órára változnak a különböző állományok, nem minden rendszereseményt naplóznak az operációs rendszerek, ráadásul rendszerbeállítástól és a használt programok beállításától függ az előzmények esetleges törlése. Több hónap elteltével szinte kizárt, hogy megállapítható lenne adott számítógép meghatározott nap szerinti állapota. Ha pedig a számítógépen az operációs rendszer újratelepítése megtörtént, akkor – a telepítés módjától függően – akár teljességgel lehetetlenné is válik egy korábbi állapot feltárása. Az eljáró tanács álláspontja szerint a Kérelmező helyesen járt el akkor, amikor a jelen üggyel érintett vitás esetet követően számítógépének újratelepítése mellett döntött.

Az eljáró tanács álláspontja szerint az xxx vírus tulajdonságaira tekintettel a Kérelmező számítógépének állapota nem releváns az ügy megítélésében. A pénzügyi szolgáltató maga nyilatkozta, hogy az xxx blokkolja a vírusvédelmi szoftvert, valamint elérhetetlenné teszi azok frissülését. A Kérelmező tehát nem volt – nem lehetett – abban a helyzetben, hogy ténylegesen védekezzen az xxx vírussal szemben.

Az eljáró tanács hangsúlyosan utal arra, hogy az xxx vírusnak, illetve annak korábbi változatainak terjedésére már több éve számos adat és tény érhető el az interneten, ezért a pénzügyi szolgáltató akkor tanúsította volna az általában elvárható magatartást, ha aaa-án nem éri őt – az eljáró tanács álláspontja szerint – „váratlanul” az xxx vírus támadása. Az eljáró tanács álláspontja szerint a pénzügyi szolgáltatónak fel kellett volna készülnie arra, hogy egy kifejezetten internetbanki csalásokra specializált vírus az ő ügyfeleit is elérheti, és nem aaa-t követően kellett volna vizsgálódnia az ügyfeleinél, akiket elért a támadás. A pénzügyi szolgáltató ugyanis úgy nyilatkozott, hogy ezen a napon érkezett hozzá az első ügyfélbejelentés, amelyet követően ügyfelei gépének helyszíni vizsgálata után megállapította, hogy az xxx vírus áll a háttérben. Az eljáró tanács nyilvánvalóan nem azt várja el a pénzügyi szolgáltatótól, hogy valamennyi vírust, illetve azok tulajdonságait ismerje, kövesse nyomon stb., de az általában elvárható a pénzügyi szolgáltatóktól, hogy azoknak a vírusoknak az alapvető működési mechanizmusát ismerjék, amelyek az internetbanki támadásokat hajtják végre, és e vonatkozásban legyenek felkészültek, illetve vezessenek be kellő időben olyan megkerülhetetlen biztonsági lépéseket, amelyekkel megvédhetik ügyfeleik pénzét.

Az eljáró tanács utal a Pénzügyi Békéltető Testület előtt folyamatban volt és a H-PBT-H-992/2013 számú határozattal lezárt ügyre, melynek tárgya egy vírusos gépről indított internetbanki átutalás volt. Abban az ügyben a kérelmező tranzakciót jóváhagyó SMS-es kóddal megerősítette az átutalási megbízást, így a Pénzügyi Békéltető Testület százszázalékos kérelmezői közrehatás miatt az eljárást a kérelem megalapozatlansága miatt megszüntette. Az eljáró tanács megjegyzi, hogy abban az ügyben az érintett pénzügyi szolgáltató nem utalt arra, hogy a tényállás megállapításához, illetve az ügy megítéléséhez szakértőre lenne szükség, holott a jelen ügyhöz teljesen hasonló informatikai kérdések merültek fel.

Az eljáró tanács a pénzügyi szolgáltató által becsatolt okirat alapján az interneten fellelhető több nyilvános információforrásból (keresőprogram, IP-címeket listázó honlap) is meggyőződött arról, hogy jelen ügyben a vitatott tranzakciót egy xxx-i IP-címről kezdeményezték. Az eljáró tanács álláspontja szerint a pénzügyi szolgáltatónak lett volna, illetve lenne lehetősége ugyanolyan „védelmi vonalat" kiépítenie az internetbanki szolgáltatásához, mint amilyet a bankok köztudottan a bankkártyák biztonságos használatához üzemeltetnek. Mindez azt jelenti, hogy meghatározott adatok, körülmények és események kapcsán a rendszer kiszűri a „gyanús" műveleteket, és akár emberi beavatkozással, akár anélkül, automatizáltan bizonyos biztonsági intézkedéseket léptetne életbe rövidebb vagy hosszabb időtartamra. A pénzügyi szolgáltató arra utalt, hogy IP-címtartományok esetén ez aggályos lehet, hiszen a változó IP-című felhasználók esetén, amikor az IP-cím kiosztása újra és újra megtörténik, egy feketelistás IP-címet megkaphat egy másik felhasználó is, akinek így a pénzügyi szolgáltató irányába blokkolva lesz a kommunikációja. A pénzügyi szolgáltató arra is utalt, hogy amikor egy-egy nagyobb szervezet sok számítógépe például egy szerveren keresztül kommunikál az internettel, így az összes gép kifelé egy IP-címnek látszik, és ha valamelyik gépről gyanús tevékenységet észlelne a pénzügyi szolgáltató rendszere, méltánytalan lenne annak az IP-címnek a kitiltása, mert így az összes többi számítógépről is elérhetetlenné válna a pénzügyi szolgáltató internetes felülete. Az eljáró tanács tudomásul veszi a pénzügyi szolgáltató aggályait az IP-címek szűrésével kapcsolatban, ugyanakkor utal a következőkre. A pénzügyi szolgáltató által megfogalmazott aggályok egy nagyon „nyers" IP-címszűrést jelentenek, hiszen annak számtalan – különösen időbeli – paramétere lehet, így egy-egy kitiltás lehet pár órás, de akár csak pár perces is. Az eljáró tanács utal arra, hogy nem önmagában az IP-címszűrés jelenthetne (illetve jelenthetett volna) a megfelelő megoldást a pénzügyi szolgáltató számára, hanem egy olyan komplex, az internetbankolásra vonatkozó csalásfelismerő- és kezelő rendszer, amelynek egyik szignifikáns komponense lehet az IP-címszűrés, melyet további olyan metódusokkal (pl. az ügyfelek internetbankolási szokásai – honnan szokta elérni az internetbankot, mennyi időn keresztül használja stb.) lehet kombinálni, amelyek – ha nem is 100%-os biztonsággal, de – nagy eséllyel kiszűrik a csalásgyanús eseteket. Ha pedig ilyen eseményre figyelmeztet a rendszer, azt akár egy telefonhívással is lehet tisztázni, ahogyan ezt bankok megteszik bizonyos esetekben (pl. külföldi bankkártya-használat esetén). A Pénzügyi Békéltető Testületnek nem feladata, hogy bármely pénzügyi szolgáltató rendszerére vonatkozóan fejlesztési javaslatot tegyen, ugyanakkor – és jelen ügyben különösen – fontos, hogy az eljáró tanács megvizsgálja, hogy a pénzügyi szolgáltató az általában elvárható módon mindent megtett-e annak érdekében, hogy ügyfeleinek a pénzét az internetbankolás során is biztonságban tartsa.

Az eljáró tanács nem osztotta a pénzügyi szolgáltatónak azt az álláspontját, mely szerint „a pénzügyi szolgáltató álláspontja szerint az IP-cím személyes adatnak minősül, amennyiben az az ügyfélre visszakövetkeztethető, ezért az érintett ügyfél tudomása nélkül annak átadása más bank felé illegális tevékenység is lehet”. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § (2) pontja szerint személyes adat az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. Az IP-cím egy hálózatba kötött számítógépet azonosít, azt azonban nem azonnal és nem minden kétséget kizáróan, hogy ténylegesen ki használja adott időpillanatban a számítógépet. Nyilvánvalóan nem kizárt, hogy IP-cím alapján utólag – bármilyen hatósági vagy bírósági ügyben egy bizonyítási eljárás során – azonosítható legyen az, hogy meghatározott időpontban ki használta az adott számítógépet, ugyanakkor általánosságban semmiképpen sem lehet kijelenteni azt, hogy az IP-cím azonnal és minden kétséget kizáróan azonosítja a felhasználó személyét. Erre vonatkozóan maga a pénzügyi szolgáltató tett előadást a vállalati tűzfalat alkalmazó rendszerek, illetve proxyszerverek tekintetében, hiszen – ahogyan az eljáró tanács arra a fentiekben is utalt – ilyen esetben többszáz vagy akár többezer felhasználó az internet „felé” egy IP-címnek látszik. Az eljáró tanács álláspontja szerint ilyen esetben még arra sem lenne szükség, hogy az ilyen technikai megoldást alkalmazó szervezettől kellene hozzájáruló nyilatkozatot beszerezni az IP-cím rögzítése miatt, hiszen köztudott, hogy szinte minden internetes honlap készít látogatottsági statisztikát, amelynek egyik nélkülözhetetlen eleme a látogatók IP-címeinek rögzítése. Összegezve tehát az eljáró tanács álláspontja az, hogy az IP-cím nem minősül személyes adatnak, illetve annak rögzítése, figyelése – egy komplex, csalásfigyelő rendszer keretében – sokkal inkább az ügyfelek elhelyezett betéteinek védelmét szolgálja, nem pedig a személyes adatokat sérti.

Az eljáró tanács álláspontja szerint a pénzügyi szolgáltató üzleti döntése volt, hogy a tranzakciónkénti kötelező SMS-es azonosítást yxz napjától vezeti csak be tekintettel a zxy „sűrű” internetbanki forgalomra. Az eljáró tanács a pénzügyi szolgáltatónak ezt a magatartását úgy értékelte, hogy a pénzügyi szolgáltató a reputációs kockázat miatt nem döntött úgy, hogy azonnal bevezeti az SMS-es azonosítást, ha pedig a pénzügyi szolgáltató drasztikusabb megoldást választ (például meghatározott időszakra – a szükséges intézkedések megtételéig – leállítja az internetbankot), azzal feltehetően rendkívüli reputációs kockázatot vállalt volna. Az eljáró tanács álláspontja szerint nem elfogadható a pénzügyi szolgáltatónak az az álláspontja, mely szerint a sikeres bejelentkezések, illetve tranzakciók magas számához képest nagyon alacsony a vírusfertőzött számítógépeken keresztül végrehajtott tranzakciók száma. Az eljáró tanács véleménye szerint ha a pénzügyi szolgáltató azt az üzleti döntést hozta, hogy a zxy elején bekövetkezett vírustámadást követően elegendő ügyfeleinek újabb figyelmeztetése, illetve csak yxz napjával vezet be szigorúbb biztonsági intézkedést, akkor egyúttal tisztában kellett lennie azzal, hogy bizonyos ügyfeleinek a pénze nem lesz biztonságban a kérdéses időszakban. Az eljáró tanács álláspontja szerint ezért az üzleti döntésért a pénzügyi szolgáltatónak helyt kell állnia, hiszen a pénzügyi szolgáltató nem tette meg az általában elvárható intézkedéseket ügyfelei pénzének védelme érdekében. Az eljáró tanács véleménye szerint zxy-ban az interneten megjelentetett figyelmeztetés nem volt

elegendő, ez tehát nem merítette ki a pénzügyi szolgáltató részéről az általában elvárható magatartás tanúsítását.

Az eljáró tanács nem osztotta a pénzügyi szolgáltatónak azt az álláspontját, mely szerint „bármely típusú xxx beállítása biztosítja ügyfeleinek a védelmét, ha a megfelelő számítástechnikai védelmet is alkalmazzák". Az ügyfelek védelmét szolgáló rendszert minden esetben a kényelem (felhasználóbarát kialakítás, könnyű kezelhetőség) és a lehetséges külső és belső rendszerkockázatok összehasonlításával kell kialakítani. Jelen vitás ügyben a pénzügyi szolgáltató üzleti döntése alapján a kényelem oldalára billent mérleg nem csak a többször említett zxy időszak, hanem yxz-ét megelőzően több év vonatkozásában is. Ez tehát azt jelenti, hogy a pénzügyi szolgáltató az internetbanki szolgáltatását kevésbé biztonságos módon is engedte használni az ügyfeleinek elégedettsége érdekében annak ellenére, hogy az xxx vírusnak (vagy esetlegesen más, rosszindulatú programnak) kiszolgáltatott ügyfeleinek a pénze nem volt kellően védve.

Az eljáró tanács utal a pénzügyi szolgáltató előadására, mely szerint „ügyfelei jelentős többsége ragaszkodik az internet által adott „szabadsághoz" és saját döntéshozatali lehetőségeikhez", a következő észrevételt teszi. A pénzügyi szolgáltató – a kényelem rovására, ugyanakkor a biztonságos internetbankolás előmozdítása érdekében – akkor tanúsította volna az általában elvárható magatartást, ha nem kizárólag az internetbankolás biztonsági kérdéseinek ismertetésére szorítkozott volna, hanem már zxy-nál jóval korábban felkészül a lehetséges internetes visszaélésekre, és az emiatt bevezetett magasabb biztonsági követelmények szükségességéről (például a tranzakciónkénti kötelező SMS-es jóváhagyásról), illetve azok kötelező voltáról – ennek folyományaként az esetlegesen kényelmetlenebb vagy lassabb internetbankolásról – tájékoztatja ügyfeleit.

Az eljáró tanács utal arra, hogy ha az ügyfél a tranzakció elindítása előtt a tranzakciót megerősítő SMS-ben értesül arról, hogy mekkora összeg melyik számlaszámra történő utalására fog sor kerülni, és a tranzakciót jóváhagyja, akkor az esetleges kár bekövetkezésében 100%-os közrehatása állapítható meg. (H-PBT-H-992/2013). Az eljáró tanács álláspontja szerint ha az ügyfél számítógépét xxx vírus fertőzi meg, akkor tranzakciónkénti SMS-es jóváhagyás (megerősítés) hiányában az internetbankot éppen használó ügyfél a belépést követően ténylegesen nem dönthet egy-egy tranzakció kezdeményezéséről, illetve nincs eszköz a kezében arra, hogy a kezdeményezett tranzakció vonatkozásában dönthessen annak végrehajtásáról, vagy – észlelve a visszaélést – úgy döntsön, hogy a tranzakciót nem erősíti meg.

Az eljáró tanács hangsúlyosan utal a következőkre. A pénzügyi szolgáltató előadása szerint ő igyekezett minden szükséges információt biztosítani az ügyfeleinek, ennek keretében a honlapján külön oldalt készített az internetbank biztonsági tudnivalóiról, és itt a Pénzügyi Szervezetek Állami Felügyeletének ajánlásaira is hivatkozik. Ez valóban így van, az yyy internetes címen („xxx internetes szolgáltatás használatához") olvashatók a pénzügyi szolgáltató információi, így az is, hogy leírásuk összhangban áll a Pénzügyi Szervezetek Állami Felügyeletének módszertani útmutatójával. A „Pénzügyi Szervezetek Állami Felügyeletének módszertani útmutatójával" a honlapon kattintható hivatkozásként szerepel, és

ez az xxx.pdf internetes címre mutat, mely dokumentum a Pénzügyi Szervezetek Állami Felügyeletének 7/2011. számú módszertani útmutatója az internetbanki szolgáltatások biztonságáról címet viseli. E dokumentum szerint a felügyeleti ajánlásban az előremutató gyakorlatként feltüntetett ajánlások hatóköre az intézmények internetbanki rendszerére terjed ki, és magában foglalja az intézmények internetbank hálózati környezetének valamennyi rendszerelemét. A 4. oldal tanúsága szerint előremutató gyakorlat az, hogy a „felsővezetés a felelősségi körében gondoskodik arról, hogy a hitelintézet csalásfelderítő – fraud monitoring – rendszert működtet az internetbank használatában előfordulható visszaélések visszaszorítására." A pénzügyi szolgáltató által előadottakból egyértelműen kiderül, hogy ő ilyen rendszert egyáltalán nem működtet, sőt annak kialakítását nem is tartja indokoltnak, illetve megvalósíthatónak.

Az eljáró tanács hangsúlyosan utal arra, hogy a második meghallgatáson feltett öt kérdés közül a pénzügyi szolgáltató a belső informatikai ellenőrzéssel, illetve belső ellenőrzéssel kapcsolatban nem adott érdemi választ, mivel csak annyit írt, hogy rendszereik „folyamatos felügyelet alatt vannak, és a védelmi eszközökön az érintett időszakban sem észlelt eredményes támadást". Ugyanakkor a pénzügyi szolgáltató a harmadik meghallgatáson úgy nyilatkozott, hogy „aaa-án érkezett hozzánk az első panasz, ekkor elkezdtük vizsgálni saját rendszereinket", ami az eljáró tanács álláspontja szerint azt jelenti, hogy a pénzügyi szolgáltatónál lehetett belső informatikai ellenőrzés az esettel kapcsolatban különös tekintettel arra, hogy a zxy-i vírustámadása vezetett végül oda, hogy a pénzügyi szolgáltató yxz-én kötelező jelleggel bevezette a tranzakciónkénti kötelező SMS-es megerősítést. Az eljáró tanács a pénzügyi szolgáltató terhére értékelte, hogy a feltett kérdésekre nem adott konkrét választ, és azokra vonatkozóan okirati bizonyítékot sem nyújtott be, illetve az írásbeli és a szóbeli előadása ellentmondásos volt.

A Ptk. 530. § bekezdése szerint betétszerződés alapján a pénzintézet köteles a szerződő fél által lekötött pénzeszközök után kamatot fizetni és a betét összegét a szerződés szerint visszafizetni.

A Hpt 50. § (1) bekezdése szerint banktitok minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.

A Ptk. 318. § (1) bekezdése alapján a szerződésszegésért való felelősségre, valamint a kártérítés mértékére a szerződésen kívül okozott károkért való felelősség szabályait kell alkalmazni azzal az eltéréssel, hogy a kártérítés mérséklésének - ha a jogszabály kivételt nem tesz - nincs helye.

A Ptk. 339. § (1) bekezdése alapján aki másnak jogellenesen kárt okoz, köteles azt megtéríteni. Mentesül a felelősség alól, ha bizonyítja, hogy úgy járt el, ahogy az az adott helyzetben általában elvárható.

A Ptk. 355. § (1) bekezdése szerint a kárért felelős személy köteles az eredeti állapotot helyreállítani, ha pedig az nem lehetséges, vagy a károsult azt alapos okból nem kívánja, köteles a károsult vagyoni és nem vagyoni kárát megtéríteni.

Az eljáró tanács álláspontja szerint a pénzügyi szolgáltató jogellenes és felróható magatartása abban áll, hogy a pénzügyi szolgáltató nem tanúsította az általában elvárható magatartást ügyfelei – jelen vitás ügyben a Kérelmező – nála elhelyezett pénze, betétje védelme érdekében. Az eljáró tanács véleménye szerint a pénzügyi szolgáltató felelőssége annak az eldöntése, hogy az általa az ügyfelei részére kínált, illetve biztosított internetes szolgáltatás vonatkozásában melyek a kötelező biztonsági elemek, illetve lépések, amelyeken az ügyfeleinek kötelező végighaladniuk az egyes tranzakciók végrehajtása során. Ha a pénzügyi szolgáltató úgy dönt – márpedig zxy napjáig így volt –, hogy – üzleti megfontolásból – ügyfeleinek kényelme érdekében nem követeli meg a több lépésből álló, ugyanakkor magasabb biztonságot jelentő internetbanki használatot, akkor az ezzel járó kockázatot is viselnie kell. Az eljáró tanács az internetbankos csalásokkal kapcsolatos védelmi vonal kiépítésével (például a fent részletezett IP-címszűréssel) kapcsolatban utal arra, hogy a pénzügyi szolgáltató az általa a honlapján is meghivatkozott felügyeleti ajánlásban foglalt internetbanki csalást észlelő rendszer működtetésével ellensúlyozhatta volna az általa – az ügyfelek vonatkozásában – alacsonyabb követelményekkel üzemeltetett internetbanki rendszert.

Az eljáró tanács osztotta a Kérelmezőnek azt az álláspontját, mely szerint a pénzügyi szolgáltató megsértette a Ptk. 530. §-át. Az eljáró tanács véleménye szerint a pénzügyi szolgáltató azt a látszatot keltheti honlapjának látogatóiban, hogy internetbanki csalásfelderítő rendszert üzemeltet, holott védelmi rendszere – a fentiekben kifejtettek alapján – saját informatikai eszközeinek védelmére szorítkozik, de az interneten történő csalásgyanús események kiszűrésére alkalmas rendszere nincs. Az eljáró tanács megállapította, hogy a pénzügyi szolgáltató a Kérelmező banktitkát sem védte meg, hiszen a Kérelmezőnek bankszámlatitka kiderült, sőt a pénzügyi szolgáltatónál elhelyezett pénze (betétje) sem volt biztonságban.

Az eljáró tanács álláspontja szerint a pénzügyi szolgáltató fentiekben kifejtett jogellenes magatartása – ideértve a részletesen kifejtett üzleti döntés körülményeit –, illetve mulasztása – internetbanki csalásfigyelő rendszer hiánya – okozati összefüggésben áll azzal, hogy a Kérelmezőt kár érte. A Pénzügyi Békéltető Testület előtti, pénzügyi fogyasztói jogvita rendezésére irányuló eljárásban a pénzügyi szolgáltató nem bizonyította, hogy a Kérelmező személyes adatainak, pénzének, illetve banktitkának megőrzése érdekében úgy járt volna el, ahogyan az az adott helyzetben általában elvárható. Mindezek alapján a pénzügyi szolgáltatónak az eredeti állapotot helyre kell állítania.

A Psztv. 94. § b) pontja alapján egyezség hiányában a tanács az ügy érdemében ajánlást tesz, ha a kérelem megalapozott, azonban a 4. §-ban meghatározott törvények hatálya alá tartozó szervezet vagy személy az eljárás kezdetekor úgy nyilatkozott, hogy a tanács döntését kötelezésként nem ismeri el, illetve ha a tanács döntésének elismeréséről egyáltalán nem nyilatkozott.

A fentiek alapján a Pénzügyi Békéltető Testület eljáró tanácsa a rendelkező részben foglaltak szerinti ajánlást tette.

Budapest, 2013. július 25.

dr. Gáll Tamás s.k., az eljáró tanács tagja	dr. Bukta Krisztina s.k., az eljáró tanács elnöke	Prihoda Anikó s.k., az eljáró tanács tagja