F i n a n č n í a r b i t r

Legerova 1581/69, 110 00 Praha 1 – Nové Město
Tel. 257 042 094, e-mail: arbitr@finarbitr.cz
www.finarbitr.cz

Evidenční číslo:
FA/11537/2015
Spisová značka (uvádějte vždy v korespondenci):
FA/PS/542/2014

N á l e z

Finanční arbitr příslušný k rozhodování sporů podle § 1 zákona č. 229/2002 Sb., o finančním arbitrovi, ve znění pozdějších předpisů (dále také „zákon o finančním arbitrovi"), rozhodl v řízení zahájeném dne 12. 11. 2014 podle § 8 zákona o finančním arbitrovi o návrhu navrhovatele [redacted], zastoupeného na základě plné moci ze dne 27. 10. 2014 Mgr. Robertem Plickou, advokátem se sídlem Národní 58/32, 110 00 Praha 1 – Nové Město, ev. č. ČAK 14849 (dále jen „Navrhovatel"), proti instituci Fio Banka, a.s., IČO 618 58 374, se sídlem V Celnici 1028/10, 117 21 Praha 1, zapsané v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka B 2704 (dále jen „Instituce"), vedeném podle § 24 zákona o finančním arbitrovi podle tohoto zákona s přiměřeným použitím zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „správní řád"), o vrácení částky ve výši 95.122 Kč s příslušenstvím, takto:

Návrh se podle § 15 odst. 1 zákona o finančním arbitrovi zamítá.

O d ů v o d n ě n í :

1. Předmět řízení před finančním arbitrem a zkoumání podmínek řízení

Návrhem se Navrhovatel proti Instituci domáhá vrácení peněžních prostředků ve výši částky platební transakce, kterou Instituce provedla na základě platebního příkazu zadaného z internetového bankovnictví Navrhovatele a kterou Navrhovatel neautorizoval, včetně úroků z prodlení z této částky.

Finanční arbitr při zkoumání podmínek řízení zjistil, že Navrhovatel uzavřel s Institucí dne 14. 6. 2013 Smlouvu o běžném účtu (dále jen „Smlouva o účtu"), na základě které mu Instituce zřídila běžný účet č. [redacted] (dále jen „Účet"), a Smlouvu o elektronické správě účtů (dále jen „Smlouva o elektronickém bankovnictví"), na základě které mu Instituce zřídila službu internetového bankovnictví. Navrhovatel s Institucí uzavřel dne 21. 1. 2014 Protokol o nastavení autorizace elektronických pokynů k účtu [redacted], ve kterém za osobu oprávněnou nakládat s Účtem označili [redacted] (dále jen „Jednatel Navrhovatele"). Jednatel Navrhovatele uzavřel s Institucí dne 21. 1. 2014 Smlouvu o elektronické správě účtů (dále jen „Smlouva o elektronickém bankovnictví s Jednatelem Navrhovatele"), na základě které mu Instituce umožnila s Účtem prostřednictvím internetového bankovnictví nakládat.

Smlouva o účtu označuje ve svém čl. II odst. 2 za svou nedílnou součást Obchodní podmínky pro zřizování a vedení účtů, v tomto případě platné od 1. 3. 2013 (dále jen „Podmínky vedení účtů z 1. 3. 2013“); Smlouva o elektronickém bankovnictví označuje ve svém čl. I. odst. 3. za svou nedílnou součást Obchodní podmínky pro zřizování a vedení účtů, v tomto případě účinné od 1. 3. 2013 (tedy Podmínky vedení účtů z 1. 3. 2013), a Obchodní podmínky pro elektronickou správu účtů, v tomto případě ze dne 18. 6. 2012 (dále jen „Podmínky elektronického bankovnictví z 18. 6. 2012“).

Smlouva o elektronickém bankovnictví a Podmínky vedení účtů z 1. 3. 2013 a Podmínky elektronického bankovnictví z 18. 6. 2012 upravují mimo jiné správu Účtu prostřednictvím internetového bankovnictví (které označuje za internetbanking) a mobilního bankovnictví (které označuje za smartbanking).

Podle čl. I odst. 1 Smlouvy o účtu se Instituce zavázala zřídit a vést Navrhovateli běžný účet, v tomto případě Účet. Podle čl. XIII. „Platební styk a zúčtování“, odst. 2 Podmínek vedení účtů z 1. 3. 2013 se Instituce zavázala přijímat v souladu s Podmínkami vedení účtů z 1. 3. 2013 na Účet vklady a platby v měně Účtu a uskutečňovat z něho v této měně výplaty a platby, pokud to vyplývá z uzavřené smlouvy. Ve Smlouvě o účtu si strany sporu v čl. XVIII „Některé informace o platebních službách“, odst. 4 Podmínek vedení účtů z 1. 3. 2013 sjednaly, že předmětem smluv, na základě kterých se poskytují platební služby, je zejména vedení běžného (platebního) účtu, provádění platebního styku, a dále případně elektronická správa běžného (platebního) účtu (internetbanking) a možnost vydání platební karty.

Pokud jde o relevantní právní úpravu, Smlouva o účtu byla do 31. 12. 2013 smlouvou o běžném účtu podle § 708 an. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů, resp. ve znění účinném do 31. 12. 2013, a od 1. 1. 2014 je smlouvou o účtu podle § 2662 an. zákona č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník“). Současně je Smlouva o účtu společně se Smlouvou o elektronickém bankovnictví rámcovou smlouvou o platebních službách podle § 74 odst. 1 písm. a) zákona č. 284/2009 Sb., o platebním styku, ve znění pozdějších předpisů (dále jen „zákon o platebním styku“), neboť Instituce se zavázala provádět pro Navrhovatele platební transakce ve smlouvě předem neurčené. Smluvní vztah mezi Navrhovatelem a Institucí je vztahem mezi uživatelem platebních služeb a poskytovatelem platebních služeb.

Dále pak, Účet je platebním účtem podle § 2 odst. 1 písm. b) zákona o platebním styku, neboť slouží k provádění platebních transakcí podle § 2 odst. 1 písm. a) zákona o platebním styku bez dispozičních omezení, tj. ke vkladům na platební účet, výběrům z platebního účtu a převodům.

Podmínky vedení účtů z 1. 3. 2013 ve svém čl. I „Předmět úpravy“, odst. 4 stanoví: *„Banka* (tedy Instituce – pozn. finančního arbitra) *je oprávněna navrhnout klientovi* (tedy Navrhovateli – pozn. finančního arbitra) *změnu smlouvy, na základě které provádí klient platební styk (např. smlouva o běžném účtu nebo Fio konto), a těchto obchodních podmínek (včetně Ceníku), (dále také „návrh na změnu smlouvy“). Návrh na změnu smlouvy se klientovi poskytuje alespoň 2 měsíce před předpokládanou účinností změny smlouvy, a to prostřednictvím internetbankingu, pokud ho má klient zřízen, nebo se klientovi poskytne osobně na úřadovně banky, která mu vede účet. Návrh na změnu smlouvy se stává pro klienta závazný, jestliže byl návrh poskytnut klientovi způsobem a ve lhůtě podle předchozí věty, klient návrh na změnu smlouvy neodmítl, ačkoli byl o tom v souvislosti s návrhem poučen a smlouvu nevypověděl, ačkoli byl o tom v souvislosti s návrhem poučen.“* Podmínky elektronického bankovnictví z 18. 6. 2012 ve svém čl. XVII. „Závěrečná ustanovení“, odst. 1 stanoví: *„V zájmu zlepšení kvality služeb poskytovaných klientovi, v souvislosti se změnou identifikace (fingerprintu) serveru banky, v návaznosti na vývoj právního prostředí a také s ohledem na obchodní politiku banky je banka oprávněna tyto Podmínky měnit a doplňovat (vyhlašovat nové znění). Banka je oprávněna navrhnout klientovi*

změnu smlouvy o elektronické správě účtu a těchto obchodních podmínek (dále také „návrh na změnu smlouvy“). Návrh na změnu smlouvy se klientovi poskytuje alespoň 2 měsíce před předpokládanou účinností změny, a to prostřednictvím internetbankingu. Návrh na změnu smlouvy se stává pro klienta závazný, jestliže byl návrh poskytnut klientovi způsobem a ve lhůtě podle předchozí věty, klient návrh na změnu smlouvy neodmítl, ačkoli byl o tom v souvislosti s návrhem na změnu smlouvy poučen a smlouvu o elektronické správě účtu nevypověděl, ačkoli byl o tom v souvislosti s návrhem na změnu smlouvy poučen. Klient je oprávněn návrh na změnu smlouvy odmítnout a smlouvu vypovědět, jestliže mu nebyla změna poskytnuta alespoň 2 měsíce před předpokládanou účinností změny.“

Podle § 94 odst. 1 zákona o platebním styku *„[n]avrhuje-li poskytovatel uživateli změnu rámcové smlouvy, musí tak učinit na trvalém nosiči dat způsobem uvedeným v § 80 odst. 1 nejpozději 2 měsíce přede dnem, kdy má podle návrhu změna rámcové smlouvy nabýt účinnosti.“* Podle § 80 odst. 1 zákona o platebním styku *„[t]yto informace musí být uživateli poskytnuty určitě a srozumitelně v úředním jazyce státu, v němž je platební služba nabízena, nebo v jazyce, na kterém se strany dohodnou.“* Trvalým nosičem dat je podle § 1 odst. 3 písm. i) zákona o platebním styku *„[j]akýkoli předmět, který umožňuje uživateli uchování informací určených jemu osobně tak, aby mohly být využívány po dobu přiměřenou účelu těchto informací, a který umožňuje reprodukci těchto informací v nezměněné podobě.“* Podle § 94 odst. 3 zákona o platebním styku *„[b]ylo-li to dohodnuto, platí, že uživatel návrh na změnu rámcové smlouvy přijal, jestliže a) poskytovatel navrhl změnu rámcové smlouvy nejpozději 2 měsíce přede dnem, kdy má změna nabýt účinnosti, b) uživatel návrh na změnu rámcové smlouvy neodmítl, c) poskytovatel v návrhu na změnu rámcové smlouvy uživatele o tomto důsledku informoval, d) poskytovatel v návrhu na změnu rámcové smlouvy informoval uživatele o jeho právu vypovědět rámcovou smlouvu podle odstavce 4.“* Podle § 94 odst. 4 zákona o platebním styku *„[j]estliže uživatel návrh na změnu rámcové smlouvy v případě uvedeném v odstavci 3 odmítne, má právo rámcovou smlouvu přede dnem, kdy má změna nabýt účinnosti, bezúplatně a s okamžitou účinností vypovědět.“*

Instituce předložila finančnímu arbitrovi přehled a obsah zpráv, které zobrazila Navrhovateli v internetovém bankovnictví. Finanční arbitr zjistil, že Instituce v souladu s § 94 zákona o platebním styku, s čl. 1 „Předmět úpravy“, odst. 4 Podmínek vedení účtů z 1. 3. 2013 a s čl. XVII. „Závěrečná ustanovení“, odst. 1. Podmínek elektronického bankovnictví z 18. 6. 2012 navrhla dne 31. 3. 2014 Navrhovateli změnu podmínek vedení účtů a podmínek elektronického bankovnictví s účinností od 2. 6. 2014. Z podkladů, které finanční arbitr shromáždil, nezjistil, že by Navrhovatel tento návrh odmítl. Finanční arbitr proto pro účely tohoto řízení považuje za součást Smlouvy o účtu Obchodní podmínky pro zřizování a vedení účtů účinné od 2. 6. 2014 (dále též „Podmínky vedení účtů“) a za součást Smlouvy o elektronickém bankovnictví Podmínky vedení účtů a Obchodní podmínky pro elektronickou správu účtů účinné od 2. 6. 2014 (dále jen „Podmínky elektronického bankovnictví“).

Součástí Smlouvy o účtu tedy byly od 14. 6. 2013 do 1. 6. 2014 Podmínky vedení účtů z 1. 3. 2013 a od 2. 6. 2014 Podmínky vedení účtů. Součástí Smlouvy o elektronickém bankovnictví pak byly od 14. 6. 2013 do 1. 6. 2014 Podmínky elektronického bankovnictví z 18. 6. 2012 a Podmínky vedení účtů z 1. 3. 2013 a od 2. 6. 2014 Podmínky vedení účtů a Podmínky elektronického bankovnictví.

Internetové bankovnictví, prostřednictvím kterého Navrhovatel Účet spravoval, je platebním prostředkem podle § 2 odst. 1 písm. d) zákona o platebním styku, neboť se jedná o *„zařízení nebo soubor postupů dohodnutých mezi poskytovatelem* (platebních služeb – pozn. finančního arbitra) *a uživatelem* (platebních služeb – pozn. finančního arbitra)*, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz“*.

Platební transakce provedená prostřednictvím aplikace internetového bankovnictví je platební transakcí podle § 3 odst. 1 písm. c) bod 3. zákona o platebním styku nebo § 3 odst. 1 písm. d) bod 3. zákona o platebním styku (tj. převod peněžních prostředků z platebního účtu).

Navrhovatel tak vystupuje vůči Instituci jako plátce podle § 2 odst. 3 písm. a) zákona o platebním styku, neboť z jeho Účtu jako platebního účtu byly peněžní prostředky, které jsou předmětem tohoto sporu, odepsány. Poskytovatelem platebních služeb plátce je pak v tomto případě Instituce.

K rozhodování sporu mezi Navrhovatelem a Institucí je finanční arbitr příslušný, neboť se jedná o spor mezi poskytovatelem platebních služeb a uživatelem platebních služeb při poskytování platebních služeb ve smyslu § 1 písm. a) ve spojení s § 3 odst. 1 a 2 zákona o finančním arbitrovi, když k rozhodování tohoto sporu je podle § 7 zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, dána pravomoc českého soudu.

4. Tvrzení Navrhovatele

Navrhovatel tvrdí, že se *„zřejmě stal obětí podvodu či počítačového pirátství“*, neboť platební příkaz k převodu peněžních prostředků ve výši 95.122 Kč z Účtu na účet č. [redacted] (dále jen „Cílový účet“) s variabilním symbolem [redacted], konstantním symbolem [redacted] a zprávou pro příjemce „prvky pro vyborni kapacity“ dne 16. 7. 2014 nezadal.

Navrhovatel popisuje, že dne 16. 7. 2014 při pokusu přihlásit se do internetového bankovnictví na svém notebooku *„obdržel výzvu k nainstalování aplikace na svůj mobilní telefon“*. Navrhovatel tvrdí, že bez provedení instalace se nemohl do internetového bankovnictví přihlásit a že *„výzva vypadala zcela věrohodně“*. Navrhovatel dále tvrdí, že *„… se pokoušel přihlásit do svého internetového bankovnictví přes webové rozhraní Instituce na svém počítači. Poté, co se objevila výzva, že je nutné, aby byly aktualizované údaje přes mobilní telefon, prostřednictvím svého mobilního zařízení tak učinil. Navrhovatel zadal své mobilní číslo na počítači a vzápětí mu přišla na mobilní telefon výzva k aktualizaci programu vydaného Institucí. Tuto akci Navrhovatel potvrdil. Po těchto provedených instrukcích se prostřednictví počítače přihlásil do internetového bankovnictví k účtu vedenému u Instituce, kde si vyřídil své finanční transakce. Ihned po skončení vyřizování plateb se Navrhovatel z internetového bankovnictví odhlásil.“*

Navrhovatel tvrdí, že asi po 10 minutách obdržel na mobilní telefon autorizační sms k platební transakci na částku 95.122 Kč a že ihned poté kontaktoval telefonicky Instituci a žádal o blokaci Účtu, neboť se domníval, že jeho notebook může být napaden virem. Instituce, resp. její zaměstnankyně, Navrhovatele ujistila, že *„peníze neodešly“*. Navrhovatel dále tvrdí, že dne 17. 7. 2014 ho Instituce telefonicky kontaktovala a sdělila mu, že *„peníze z jeho účtu odešly“*, a doporučila mu podat trestní oznámení, což Navrhovatel učinil.

Navrhovatel namítá, že současně podal reklamaci, kterou Instituce zamítla, a protest proti vyřízení reklamace, který Instituce rovněž zamítla.

Navrhovatel považuje provedený převod peněžních prostředků z Účtu na Cílový účet za neautorizovanou platební transakci, neboť k ní Navrhovatel nedal souhlas. Podle Navrhovatele *„[j]e evidentní, že platební transakci nezadával Navrhovatel, ale šlo o podvod třetí osoby, přičemž skutečný projev vůle Navrhovatele zde zcela absentoval“*. Navrhovatel dovozuje, že Instituce měla bezprostředně poté, co jí Navrhovatel oznámil, že platební transakci neprovedl, uvést Účet do stavu, v němž by byl, kdyby k jejímu odepsání nedošlo, neboť Navrhovatel ztrátu nezpůsobil svým podvodným jednáním, ani úmyslně či z hrubé nedbalosti neporušil své povinnosti stanovené v § 101 zákona o platebním styku.

Navrhovatel argumentuje, že *„[ž]ádnou ze svých povinností neporušil. Pokud by však finanční arbitr došel k závěru, že Navrhovatel nějakou povinnost porušil, Navrhovatel je přesvědčen, že zde ale minimálně nebyl splněn znak v tom, že by jednal nedbale, resp. že by jeho nedbalost byla hrubá. Pro takový závěr mimo jiné hovoří i skutečnost, že při počítačovém útoku, jehož se stal Navrhovatel obětí, byly podle všeho použity sofistikované a důvěryhodně se tvářící aplikace, že se nemohl do internetového bankovnictví přihlásit jinak než jejich využitím“*.

Navrhovatel dovozuje, že škoda ve výši 95.122 Kč vznikla následkem porušení zákonné povinnosti uložené Instituci právními předpisy. Navrhovatel se odvolává na Podání vysvětlení PČR, který učinil součástí návrhu na zahájení řízení před finančním arbitrem.

Navrhovatel tvrdí, že na počítači, který použil dne 15. 7. 2014 a 16. 7. 2014, byl nainstalovaný operační systém Windows 8, ve kterém je automaticky integrován antivirový program od společnosti Microsoft a na doporučení IT technika další antivirový program neinstaloval. Navrhovatel odkázal na webovou diskusi a internetový článek, kde je častokrát zaznamenáno, že ani další nainstalovaný antivirus (např. AVG) neobjevil vir, jehož obětí se stal Navrhovatel.

Navrhovatel tvrdí, že používal mobilní telefon značky Samsung S5, operační systém Android (dále jen „Mobilní telefon Navrhovatele“), což dokládá fakturou k nákupu mobilního telefonu. Navrhovatel na Mobilní telefon Navrhovatele neinstaloval antivirový program nad rámec standardního softwarového vybavení dodaného výrobcem, avšak jeho operační systém pravidelně aktualizoval k výzvě samotného přístroje. Navrhovatel zdůrazňuje, že veškeré aplikace, které jsou k dispozici ke stažení na portálu Google Play Store, jsou automaticky kontrolovány, jestli neobsahují škodlivý malware, pomocí služby Bouncer. Jakmile je aplikace určená koncovým uživatelům odeslána do Google Play Store, Bouncer ji kontroluje a porovnává s dosud známými malwary. Každá aplikace je spuštěna v simulačním prostředí, které odpovídá koncovým přístrojům, kde se zkoumá, zda se nechová útočně. Její chování je porovnáváno s chováním jiných škodlivých aplikací, aby se odhalila jejich případná shoda. Účty nových vývojářů se zkoumají tak, aby se předešlo opětovným registracím vyřazených vývojářů.

Navrhovatel namítá, že Instituce pochybila, když ho její zaměstnanci výslovně ujistili, že k provedení sporné platební transakce nedojde. Navrhovatel odkazuje na výroky zaměstnanců Instituce obsažené v záznamech telefonních hovorů, konkrétně jde o záznam s názvem *„[redacted]wav“*, kde jde o výroky: *„ono by to samozřejmě neodešlo, jo, ono se tam jakoby do mínusu na tom účtu nedostanete, ale už jsem vám to tady nastavil, takže to už ani autorizovat nepůjde“; „teďka máte zablokovaný ten internetbanking, aby vám nemohly být odeslány žádné platby“* a *„určitě, právě proto máme tu smsku, aby to tímto způsobem nešlo, pokud by někdo věděl vaše uživatelské jméno a heslo, obejít, jo“*. Z toho Navrhovatel dovozuje pochybení Instituce v jejím způsobu zabezpečení autorizace plateb, neboť má za to, že se nějakým způsobem lze sms autorizaci vyhnout. V záznamu s názvem *„[redacted]wav“* pak jde o výroky *„dobře, já jsem nechala pozastavit všechny platby“; „peníze z účtu odešly, ale jejich odeslání je zastavené; rozhodně nebudou odeslané na ten cílový účet“* a *„nemusíte se bát, ta platba je zablokovaná“*. Pochybení Instituce Navrhovatel spatřuje v tom, že přes maximální možnou snahu Navrhovatele a tvrzení zaměstnanců Instituce o učiněných zabezpečujících krocích Instituce spornou platební transakci realizovala.

Navrhovatel dovozuje, že pokud sám finanční arbitr *(osoba pověřená šetřením ve věci – pozn. finančního arbitra)* označil spornou platební transakci při ústním vysvětlení za neautorizovanou, musí za ni podle zákona nést Instituce odpovědnost. Navrhovatel má za to, že po ohlášení neautorizované platební transakce měla Instituce převedené peněžní prostředky z Cílového účtu *(který sama vede – pozn. finančního arbitra)* odebrat.

Navrhovatel odmítá, že by porušil povinnost používat internetové bankovnictví, jak s Institucí sjednal ve Smlouvě o elektronickém bankovnictví, neboť na počítači měl nainstalovaný operační

systém Windows 8 s integrovaným antivirovým programem společnosti Microsoft, a to s nastavenou samoinstalací veškerých stažených aktualizací.

Navrhovatel je přesvědčený, že i na Mobilním telefonu Navrhovatele antivirový program měl, a to buď ze standardního nastavení či od oddělení IT, které mu telefon konfigurovalo. Operační systém Mobilního telefonu Navrhovatele obsahuje ochranné prvky a Navrhovatel jej pravidelně aktualizoval. Ustanovení čl. XIV. Podmínek elektronického bankovnictví podle Navrhovatele nemůže jít k jeho tíži pro svou vágnost, neboť v něm nejsou stanoveny Institucí schválené konkrétní doporučené verze ochranných programů.

Navrhovatel odkazuje na existenci případů, kdy ani antivirové programy škodlivý malware nezaznamenaly, popř. jej odstranily pouze částečně. Navrhovatel dodává, že po provedení sporné platební transakce Mobilní telefon Navrhovatele kompletně vymazal a uvedl do továrního nastavení a následně aktualizoval celý operační systém. Nemůže tedy finančnímu arbitrovi předložit informaci o verzi operačního systému v době provedení Sporné platební transakce.

Pokud jde o varování doručovaná Institucí Navrhovateli do internetového bankovnictví, Navrhovatel namítá, že tyto jsou ze dne 28. 1. 2014, tedy v době provedení sporné platební transakce byly zcela neaktuální s ohledem na dynamický vývoj počítačového pirátství. Varování před útokem, jehož obětí se Navrhovatel stal při provedení neautorizované platební transakce, nadto Instituce zaslala až dne 18. 7. 2014, tedy po jejím provedení. Navrhovatel má za to, že Instituce by měla Navrhovateli tato varování zasílat na jeho e-mailovou adresu. Zprávy v internetovém bankovnictví si Navrhovatel může zobrazit až po přihlášení, tedy v případě napadení počítače až po zadání přihlašovacích údajů. Navrhovatel toto jednání Instituce považuje za hrubě nedbalé a alibistické.

Navrhovatel zdůrazňuje, že jednal v souladu se standardními obezřetnostními zásadami průměrného uživatele informačních technologií. Aplikaci určenou pro mobilní telefon stáhnul na webové adrese, která byla vzhledově totožná s přihlašovací stránkou Instituce. Instituce měla podle názoru Navrhovatele zabránit existenci takových webových stránek, a to s pomocí programu, který by takové stránky sám vyhledával a porovnával je se zadaným vzhledem, tedy stránkami Instituce. Navrhovatel tvrdí, že s hrubou nedbalostí postupovala Instituce.

Navrhovatel dovozuje, že Instituce by měla sledovat IP adresy, ze kterých uživatelé zadávají platební příkazy, neboť v případě Navrhovatele byl platební příkaz ke Sporné platební transakci zadán z jiné IP adresy, než ze které se Navrhovatel standardně přihlašuje.

Navrhovatel se domáhá proti Instituci vrácení peněžních prostředků ve výši 95.122 Kč a dále úroků z prodlení se sazbou 8,05 % p. a. z částky 95.122 Kč ode dne odepsání částky platební transakce z účtu Navrhovatele, tj. ode dne 16. 7. 2014, do zaplacení.

Navrhovatel současně tvrdí, že hodlá pouze subsidiárně využít možnosti domoci se částky sporné platební transakce, která je podle tvrzení Instituce stále uložena na Cílovém účtu, postupem podle § 81a zákona č. zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů (dále jen „trestní řád“), neboť by podle jeho názoru Instituce měla částku Sporné platební transakce Navrhovateli vyplatit a sama se připojit k trestnímu řízení jako poškozená.

Navrhovatel v řízení finančnímu arbitrovi sdělil, že je připraven celý případ medializovat, a to s ohledem *„na zavrženíhodný přístup Fio Banky ke svým klientům“* a postup finančního arbitra. Navrhovatel namítá, že řízení nebylo nestranné, když jednání před finančním arbitrem bylo konáno v sídle Instituce, ale možnost zplnomocnění finančního arbitra k nahlédnutí do trestního spisu bylo odmítnuto s odkazem na nutnost dodržování nestrannosti. Navrhovatel současně tvrdí, že v rámci trestního řízení byl kontaktován několika zástupci jiných bank, kteří potvrdili, že

všechny ostatní banky (obzvláště v situaci, kdy banky měly finance zablokované na svých účtech) škody ihned svým klientům vyplatily.

6. Tvrzení Instituce

Instituce potvrzuje, že z IP adresy [redacted] dne 16. 7. 2014 v 15:27:29 hod přijala platební příkaz k převodu částky 95.122 Kč z Účtu na Cílový účet s variabilním symbolem [redacted] a konstantním symbolem [redacted] a v 15:27:30 hod. požadavek o zaslání autorizačního sms kódu.

Instituce tvrdí, že požadovaný sms kód odeslala na telefonní číslo [redacted] v 15:27:31 hod. a v 15:29:36 hod. přijala potvrzení k provedení převodu v podobě autorizačního sms kódu. Instituce tvrdí, že peněžní prostředky ve výši 95.122 Kč odepsala z Účtu v 15:29:41 hod. a v tentýž okamžik je připsala na Cílový účet.

Instituce namítá, že opakovaně informovala Navrhovatele o hrozících nebezpečích, Navrhovatel však těmto zprávám nevěnoval pozornost. Instituce doplňuje, že informace o bezpečnostních hrozbách je možné zjistit také na jejích webových stránkách, konkrétně na přihlašovací stránce internetového bankovnictví.

Instituce tvrdí, že Navrhovatel si sám aktivně na svá elektronická zařízení nainstaloval škodlivý software, přičemž se s největší pravděpodobností jednalo o typ malware, před kterým Instituce své klienty varovala dne 11. 3. 2014 a 9. 5. 2014. Instituce namítá, že autorizační sms systém není možné obejít, jak dovozuje Navrhovatel, neboť v tomto případě šlo o zneužití autorizačního sms kódu, jehož vyzrazení způsobil Navrhovatel.

Instituce argumentuje, že nemá možnost ovlivnit kvalitu zajištění elektronických zařízení svých klientů, zejména aktualizaci a typ antivirového programu, hodnocení bezpečnosti programů/aplikací nainstalovaných do těchto zařízení, či přístup třetích osob k těmto zařízením. V situaci, kdy si klient aktivně škodlivé aplikace nainstaluje, je naprosto bezbranná.

Instituce hodnotí počínání Navrhovatele, tedy instalaci malware na jeho elektronických zařízeních a jeho ignorování zpráv zasílaných do internetového bankovnictví i standardních obezřetnostních zásad průměrného uživatele informačních technologií, jako hrubou nedbalost, která způsobila vyzrazení dvou typů personalizovaných bezpečnostních prvků platebního prostředku, tedy hesla při přístup do internetového bankovnictví a autentizačního kódu sloužícího k autorizaci provedené platební transakce.

Instituce tvrdí, že poté, co Navrhovatel oznámil, že platební transakci neautorizoval, podala oznámení podezřelého obchodu Finančnímu analytickému útvaru Ministerstva financí a že Policie České republiky následně vydala usnesení o blokaci peněžních prostředků na Cílovém účtu. Instituce nechápe, proč se Navrhovatel nepokusil tyto peněžní prostředky získat postupem podle § 81a trestního řádu.

Instituce namítá, že provedla veškerá opatření k zajištění částky ze sporné platební transakce, ale v okamžiku, kdy Navrhovatel oznámil platební transakci Instituci jako neautorizovanou, se již peněžní prostředky nacházely na Cílovém účtu, neboť oba účty vede Instituce.

Instituce namítá, že ztrátu z neautorizované platební transakce nese v tomto případě Navrhovatel podle § 116 odst. 1 písm. b) zákona o platebním styku a nikoli Instituce.

Instituce vysvětluje, že nemůže standardně sledovat, popř. blokovat platební příkazy zadané z jiné než obvyklé IP adresy uživatele, neboť mnoho jejích klientů si chrání své soukromí a využívá anonymizačních služeb (např. TOR).

Instituce tvrdí, že Navrhovatel se ode dne 14. 7. 2014 do dne 16. 7. 2014 12:07:33 hod. ani jednou nepřihlašoval do internetového bankovnictví a ani jednou nenavštívil webové stránky Instituce ze své běžné IP adresy.

8. Právní posouzení

Finanční arbitr podle § 12 odst. 1 zákona o finančním arbitrovi rozhoduje podle svého nejlepšího vědomí a svědomí, nestranně, spravedlivě a bez průtahů a pouze na základě skutečností zjištěných v souladu s tímto zákonem a zvláštními právními předpisy. Podle § 12 odst. 3 zákona o finančním arbitrovi není finanční arbitr vázán návrhem a aktivně opatřuje důkazy; při svém rozhodování vychází ze skutkového stavu věci a volně hodnotí shromážděné důkazy.

Navrhovatel se domáhá, aby mu Instituce vrátila peněžní prostředky ve výši 95.122 Kč, které zaúčtovala k tíži jeho Účtu na základě platebního příkazu, který nezadal, a to spolu s úroky z prodlení ve výši 8,05 % p.a. z částky 95.122 Kč ode dne odepsání částky platební transakce z účtu, tj. ode dne 16. 7. 2014, do zaplacení.

Finanční arbitr na základě tvrzení stran sporu a shromážděných podkladů vychází z následujících zjištění:

1) Navrhovatel dne 15. 7. 2014 nejpozději v 13:14 hod. přijal a následně otevřel připojenou přílohu zprávy elektronické pošty, přesněji e-mail s předmětem *„Exekuční příkaz* [redacted], kde je jako odesílatel (údaj *„Od“*) uveden [redacted] a jako příjemce (údaj *„Komu“*) uvedeno [redacted]; přílohou byl soubor ve formátu ZIP s názvem *„prikazFC5612B518756836F.zip“*; text tohoto e-mailu zněl: *„EXEKUČNÍ PŘÍKAZ Soudní exekutor* [redacted]*, Exekutorský úřad Plzeň – město, IČ 30080802, se sídlem Rychtaříkova 15, 150 00 Plzeň pověřený provedením exekuce: č.j. 1 XE 399/2014-14, na základě exekučního titulu: Příkaz č.j.* [redacted]*/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění označených povinností, které ukládá ustanovení, stejně ták, jako i povinnosti uhradit náklady na nařízení exekuce a odměnu soudního exekutora, případně zálohu na náklady exekuce a odměnu soudního exekutora: Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 8 763,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 594,00 Kč včetně DPH 21% Náklady exekuce paušálem: 6 267,00 Kč včetně DPH 21% Pro splnění veškerých povinností je třeba uhradit na účet soudního exekutora (č.ú.* [redacted]*, variabilní symbol* [redacted]*, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 16 624,00 Kč Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti. Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinností najdete v přiložených souborech. Za správnost vyhotovení* [redacted]*“* (dále jen „E-mail od exekutora“); to vyplývá z otisku obrazovky počítače se zobrazením e-mailové zprávy ze dne 15. 7. 2014, který finančnímu arbitrovi předložil Navrhovatel, a jeho vlastního tvrzení.

2) Dne 16. 7. 2014 v 12:07:33 hod. se Navrhovatel přihlásil do internetového bankovnictví Navrhovatele z IP adresy [redacted]; v 12:07:34 hod zkontroloval zůstatek na Účtu a v 12:14:41 hod. zadal platební příkaz, který v 12:15:10 hod. potvrdil zadáním autorizačního sms kódu. V 12:16:18 hod. zadal Navrhovatel další platební příkaz, který v 12:17:11 hod. potvrdil zadáním autorizačního sms kódu.

3) Dne 16. 7. 2014 v 12:59:39 hod. došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted] a ke kontrole zůstatku na Účtu; Navrhovatel se k tomuto přihlášení nevyjádřil, ale protože k němu došlo z jiné IP adresy, než bezprostředně předtím

použil Navrhovatel, a protože Navrhovatel neoznačuje toto přihlášení za jím provedené při výčtu událostí ze dne 16. 7. 2014, má finanční arbitr za to, že je neprovedl Navrhovatel (dále jen „Sporné přihlášení I“).

4) Dne 16. 7. 2014 v 15:24:40 hod. došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted] a v 15:24:41 hod. ke kontrole zůstatku na Účtu, které neprovedl Navrhovatel (dále jen „Sporné přihlášení II“). V 15:27:29 hod. byl zadán platební příkaz k převodu částky 95.122 Kč na Cílový účet a v 15:29:36 hod. byl potvrzen zadáním autorizačního sms kódu (dále jen „Sporná platební transakce“).

   Skutečnosti popsané v bodech 2, 3 a 4 vyplývají z tvrzení samotného Navrhovatele, podkladů, které předložila Instituce (konkrétně z Přehledu přístupů do IB, otisku informačního systému Instituce se zobrazením výpisu aktivit v internetovém bankovnictví Navrhovatele dne 16. 7. 2014, Přehledu aktivit v IB a z 2 otisků informačního systému Instituce se zobrazením informací o Sporné platební transakci).

5) Dne 16. 7. 2014 v 15:27 hod. obdržel Navrhovatel na Mobilní telefon Navrhovatele sms s textem: *„Aut.kod: [redacted] pro pokyn c.:[redacted] Typ:Jednor.plat.prikaz Z uctu:[redacted] Mnozstvi:95122.00 Mena:CZK Na ucet:[redacted] Datum:16.0…“.*

   To vyplývá z tvrzení Navrhovatele a z otisku obrazovky mobilního telefonu se zobrazením autorizačních sms, který předložil finančnímu arbitrovi Navrhovatel.

6) Dne 16. 7. 2014 v 15:29:07 hod. kontaktoval Navrhovatel telefonicky Instituci. Instituce Navrhovatele identifikovala; identifikace skončila po 38 vteřinách od začátku hovoru. Navrhovatel v tomto telefonickém hovoru označil Spornou platební transakci za neautorizovanou, telefonický hovor skončil v 15:35:59 hod.

   To vyplývá z tvrzení Navrhovatele, z podkladů, které předložila Instituce, konkrétně ze záznamu telefonického hovoru mezi Navrhovatelem a Institucí s názvem souboru „[redacted] *.wav“,* a z otisku informačního systému Instituce se zobrazením informace o datu a čase začátku a konce telefonického hovoru mezi Navrhovatelem a Institucí ze dne 16. 7. 2014, od 15:29 hod.

7) Instituce dne 16. 7. 2014 v 15:29:41 hod. provedla Spornou platební transakci, tedy odepsala peněžní prostředky ve výši 95.122 Kč z Účtu a v tentýž okamžik je připsala na Cílový účet.

   To vyplývá z 2 otisků informačního systému Instituce se zobrazením informací o Sporné platební transakci.

8) Dne 16. 7. 2014 v 15:34:29 hod. se Navrhovatel přihlásil do internetového bankovnictví Navrhovatele z IP adresy [redacted] a v 15:34:30 hod. provedl kontrolu zůstatku na Účtu.

   To vyplývá z Přehledu přístupů do IB, otisku informačního systému Instituce se zobrazením výpisu aktivit v internetovém bankovnictví Navrhovatele dne 16. 7. 2014, Přehledu aktivit v IB a z 2 otisků informačního systému Instituce se zobrazením informací o Sporné platební transakci.

9) Instituce Spornou platební transakci zúčtovala k tíži Účtu dne 16. 7. 2014.

   To vyplývá z výpisu z Účtu za měsíc červenec 2014, kde je u této platební transakce jako datum účtování i jako datum transakce uvedeno *„16.7.2014“*, jako ID operace „[redacted]“, jako

operace *„Platba převodem“*, jako zpráva pro příjemce *„prvky pro vyborni kapacity“*, jako číslo protiúčtu číslo Cílového účtu, jako variabilní symbol „[redacted]“, jako konstantní symbol „[redacted]“ a jako částka *„-95 122,00“*.

Navrhovatel tvrdí, že počítačový vir napadl jeho elektronická zařízení a finančnímu arbitrovi k tomu předložil otisk E-mailu od exekutora, který obdržel a ke kterému v Podání vysvětlení PČR tvrdí: *„na tuto adresu* ([redacted] – pozn. finančního arbitra) *mi přišel dne 15. 7. 2014 v 13:14:05 hodin email, který byl původně adresován na adresu [redacted] Jednalo se o email, který byl nazván exekuční příkaz [redacted] V e-mailu bylo uvedeno, že proti příjemci emailu je vedeno exekuční řízení, které vede [redacted] z Exekutorského úřadu Plzeň. město pod č. exe: [redacted]. […] Já jsem rozklikl přílohu tohoto emailu, která byla nazvána prikaz FC5612B518756836F.zip. Příloha se takzvaně rozbalila, na monitoru se ukázal nějaký text o exekuci. Nejsem si vědom toho, zda se do počítače něco instalovalo, nebo rozbalilo. Já jsem pak křížkem tuto přílohu uzavřel a dále jsem nic neřešil. […] K věci dále uvádím, že prvotní email byl odeslán z adresy [redacted], u které bylo uvedeno jméno [redacted]. Toto jméno bylo uvedeno i na konci emailu jako jméno odpovědné osoby.“*

Navrhovatel na jednu stranu tvrdí, že jeho elektronická zařízení byla napadena počítačovým virem, ale netvrdí, že počítačový vir představoval E-mail od exekutora. Na podporu svých tvrzení nepředložil žádné podklady, a to ani E-mail od exekutora v jeho elektronické podobě.

Navrhovatel tvrdí, že si do svého mobilního telefonu instaloval aplikaci, ke které v Podání vysvětlení PČR tvrdí: *„[p]ak jsem se následující den, tedy 16. 7. 2014 chtěl z mého počítače přihlásit na Internetové bankovnictví FIOBANK, kde má účet má společnost [redacted]. Jedná se o účet č. [redacted]. Použil jsem vyhledávač chrome, kde jsem zadal adresu Fiobanka.cz a otevřela se mi stránky banky. Tam jsem klikl na internetové bankovnictví a po zadání mých přihlašovacích údajů se mi přímo na stránce FIO banky otevřela povinná aktualizace zvyšování bezpečnosti pomocí chytrého telefonu. Byl jsem vyzván k výběru operačního systému telefonu, kdy bylo na výběr z 5-ti systémů. Já mám android a proto jsem klikl na kolonku s androidem. Pak chtěla aktualizace mé telefonní číslo, které jsem zadal. Jedná se o číslo uvedené shora* ([redacted] pozn. finančního arbitra). *Během asi 1 minuty jsem obdržel nějakou odpověď z Fiobanky. Nevím již, zda se jednalo o sms, mms nebo nějaký internetový odkaz. Telefon po mě chtěl stáhnout nějakou aplikaci tvářící se jako od Fio banky. Já jsem tak učinil a aplikace mě vyzvala k zadání mých přihlašovacích údajů do elektronického bankovnictví Fiobanky. Já jsem tak učinil a pak se aplikace ukončila. Poté jsem mohl normálně z počítače vstoupit do elektronického bankovnictví, kde jsem normálně prováděl platby a potřebné věci. […] Pokud jsem dotazován na skutečnost, zda jsem si všiml nějakých změn v počítači, nebo na stránkách Fiobanky tak uvádím, že ne. Vše mi připadlo naprosto shodné s Fiobankou s jejich stránkami. Nevšiml jsem si však pod jakou doménou byla ta aktualizace prováděna.“*

Navrhovatel finančnímu arbitrovi svůj mobilní telefon v řízení nepředložil, ačkoli k tomu byl vyzván.

Finanční arbitr v průběhu řízení opakovaně po Navrhovateli požadoval předložení všech záznamů týkajících se telekomunikačního provozu na telefonním čísle [redacted], tedy na telefonním čísle, které Navrhovatel používal k přijímání autorizačních sms, a to přehled sms zpráv přijatých na toto telefonní číslo a odeslaných z tohoto telefonního čísla ve dnech 15. 7. 2014 a 16. 7. 2014, včetně časových údajů o přijetí nebo odeslání sms a telefonního čísla odesílatele nebo příjemce, přehled IP adres, ze kterých bylo z tohoto telefonního čísla přistupováno do sítě internet ve dnech 15. 7. 2014 a 16. 7. 2014 a záznamy o stahování dat do tohoto mobilního telefonu (příp. množství stažených dat) ve dnech 15. 7. 2014 a 16. 7. 2014, včetně časových údajů. Dále finanční arbitr po Navrhovateli požadoval i záznamy týkající se tvrzeného útoku na elektronická zařízení Navrhovatele.

Některé shora uvedené záznamy si mohl opatřit Navrhovatel sám a některé mohl obsahovat trestní spis, do kterého je mohl založit sám Navrhovatel nebo si je mohl opatřit orgán činný v trestním řízení. Finanční arbitr není oprávněn vyžadovat po orgánech činných v trestním řízení takové podklady nebo informace sám, neboť zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů (dále jen „trestní řád"), je speciálním zákonem vůči zákonu o finančním arbitrovi. Ustanovení trestního řádu ani zákona o finančním arbitrovi neumožnují finančnímu arbitrovi získat informace o trestním řízení a současně není finančním arbitr osobou oprávněnou nahlížet do spisu trestního řízení podle § 65 trestního řádu.

Finanční arbitr není oprávněn takové informace vyžadovat ani od osoby, která shora uvedené záznamy uchovává, neboť zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále jen „zákon o elektronických komunikacích"), je taktéž speciálním zákonem vůči zákonu o finančním arbitrovi. Ustanovení zákona o elektronických komunikacích neumožňují finančnímu arbitrovi získávat provozní údaje ve smyslu zákona o elektronických komunikacích.

Záznamy o telekomunikačním provozu na telefonním čísle [redacted] by totiž s největší pravděpodobností umožnily prokázat okolnosti Navrhovatelem tvrzené instalace aplikace do mobilního telefonu, případně zjistit, zda a jakým způsobem se autorizační sms kód z autorizační sms dostal do dispozice třetí osoby.

Navrhovatel tyto podklady nepředložil (nejprve tvrdil, že si o ně požádal, pak požadoval, aby finanční arbitr si podklady vyžádal sám) s odůvodněním, že podle jeho informací nejsou v trestním spisu vedeny jiné záznamy o napadení elektronických zařízení Navrhovatele, než které již předložil; z toho finanční arbitr dovozuje, že obsahem trestního spisu by tedy bylo pouze Podání vysvětlení PČR bez dalších podkladů, které orgány činné v trestním řízení obvykle získají.

Podle § 120 odst. 1 zákona o platebním styku platí, že *„[j]estliže uživatel platebních služeb tvrdí, že provedenou platební transakci neautorizoval nebo že platební transakce byla provedena nesprávně, je poskytovatel platebních služeb povinen doložit, že byl dodržen postup, který umožňuje ověřit, že byl dán platební příkaz, že tato platební transakce byla správně zaznamenána, zaúčtována, a že nebyla ovlivněna technickou poruchou nebo jinou závadou"*.

Platební transakce, v tomto případě převod peněžních prostředků, je podle § 98 odst. 1 zákona o platebním styku autorizována, jestliže k ní plátce dal souhlas. Plátcem je pak ve smyslu § 2 odst. 3 písm. a) téhož zákona uživatel, z jehož platebního účtu mají být odepsány peněžní prostředky k provedení platební transakce, nebo který dává k dispozici peněžní prostředky k provedení platební transakce. Podle § 98 odst. 3 téhož zákona *„[f]orma a postup udělení souhlasu musí být dohodnuty mezi plátcem a poskytovatelem"*.

Formu a postup udělení souhlasu k platební transakci si v tomto případě dohodli Navrhovatel a Instituce v Podmínkách elektronického bankovnictví, kde podle Čl. III. „Autorizace elektronicky podaných pokynů" odst. 3. *„[a]utorizaci pokynu prostřednictvím sms kódu provádí klient uvedením zaslaného sms kódu do příslušného pole formuláře pro zadávání pokynů v rámci internetbankingu poté, co se řádně přihlásil do internetbankingu svým přihlašovacím jménem a přístupovým heslem. Je-li klientem vložený sms kód shodný s sms kódem vygenerovaným a zaslaným bankou, je pokyn autorizován."*

Instituce předložila výpis aktivit v internetovém bankovnictví Navrhovatele dne 16. 7. 2014 a Přehled aktivit v IB, které v tomto případě dokládají, že Sporná platební transakce byla provedena po úspěšném přihlášení do internetového bankovnictví Navrhovatele (to vyplývá ze záznamu *„16.7.2014 15:24 Přihlášení do aplikace Internetbanking"*) za použití autorizačního

sms kódu (to vyplývá ze záznamu *„Úspěšná autorizace pokynu SMS“*). Instituce tak prokázala, že při Sporné platební transakci byla dodržena dohodnutá forma a postup.

Přesto Navrhovatel tvrdí, že Spornou platební transakci nezadal, resp. slovy zákona o platebním styku neautorizoval.

Podle § 98 odst. 1 zákona o platebním styku může souhlas s platební transakcí platně udělit pouze plátce, v tomto případě Navrhovatel. Přítomnost souhlasu plátce je nutnou podmínkou autorizace platební transakce, a proto jestliže souhlas s platební transakcí udělí osoba od plátce odlišná bez souhlasu Navrhovatele, potom i kdyby při tom dodržela dohodnutou formu a postup, nejedná se o platební transakci autorizovanou.

To aprobuje i čl. 59 odst. 2 Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách na vnitřním trhu, kterou se mění směrnice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a zrušuje směrnice 97/5/ES, ve znění pozdějších předpisů (dále jen „Směrnice“), který stanoví, že *„[p]okud uživatel platební služby popírá autorizaci provedené platební transakce, použití platebního prostředku zaznamenané poskytovatelem platebních služeb nemusí být samo o sobě postačující pro prokázání, zda daná platební transakce byla plátcem autorizována nebo zda se plátce dopustil podvodu nebo zda z důvodu hrubé nedbalosti nebo úmyslně nesplnil jednu nebo více svých povinností podle článku 56.“*

Nadto *„[č]eský zákonodárce netransponoval výslovně čl. 59 odst. 2 směrnice o platebních službách, podle něhož použití platebního prostředku zaznamenané poskytovatelem „nemusí být samo o sobě postačující k prokázání“ autorizace nebo podvodu, úmyslu či hrubé nedbalosti na straně plátce. Citované ustanovení totiž neříká nic jiného než to, co vyplývá již ze zásady volného hodnocení důkazů, která platí jak v civilním soudním řízení, tak v řízení před finančním arbitrem…“ (Beran, J., Doležalová, D., Strnadel, D., Štěpánová, A.: Zákon o platebním styku. Komentář. 1. vydání. Praha: C. H. Beck, 2011).*

Tvrzení Navrhovatele, že Spornou platební transakci neautorizoval on sám, tedy že s ní neudělil souhlas, Instituce nevyvrátila.

Spornou platební transakci musí finanční arbitr posuzovat tedy jako platební transakci neautorizovanou, se kterou zákon o platebním styku spojuje právní následky v podobě speciální odpovědnosti poskytovatele nebo uživatele platebních služeb za neautorizovanou platební transakci.

Odpovědnost poskytovatele platebních služeb, v tomto případě Instituce, za neautorizovanou platební transakci upravuje ustanovení § 115 zákona o platebním styku, které stanoví: *„(1) Jestliže byla provedena neautorizovaná platební transakce, poskytovatel plátce neprodleně po té, co mu plátce neautorizovanou platební transakci oznámil, a) uvede platební účet, z něhož byla částka platební transakce odepsána, do stavu, v němž by byl, kdyby k tomuto odepsání nedošlo, b) vrátí částku platební transakce, včetně zaplacené úplaty a ušlých úroků, plátci, jestliže postup podle písmene a) nepřipadá v úvahu. (2) Odstavec 1 se nepoužije, jestliže ztrátu z neautorizované platební transakce nese plátce.“*

Ustanovení § 116 odst. 1 zákona o platebním styku potom upravuje případy, kdy je vyloučena nebo omezena odpovědnost poskytovatele platebních služeb, v tomto případě Instituce, za neautorizovanou platební transakci proto, že ztrátu z neautorizované platební transakce nese zcela nebo v určité výši plátce, v tomto případě Navrhovatel. Jedná se o případy, kdy je platební transakce provedena prostřednictvím platebního prostředku.

V tomto případě byla Sporná platební transakce provedena prostřednictvím aplikace internetového bankovnictví, tedy prostřednictvím platebního prostředku.

Konkrétně, podle § 116 odst. 1 písm. a) zákona o platebním styku *„[p]látce nese ztrátu z neautorizovaných platebních transakcí a) do částky odpovídající 150 eurům, pokud tato ztráta byla způsobena 1. použitím ztraceného nebo odcizeného platebního prostředku, nebo 2. zneužitím platebního prostředku v případě, že plátce nezajistil ochranu jeho personalizovaných bezpečnostních prvků“*.

Ve zbytku je ztráta z neautorizovaných platebních transakcí pokryta odpovědností poskytovatele platebních služeb plátce. V projednávaném případě připadá do úvahy pouze případ zneužití platebního prostředku, kterým je internetové bankovnictví Navrhovatele, podle § 116 odst. 1 písm. a) bodu 2 zákona o platebním styku, neboť další případy neoprávněného užití platebního prostředku, tj. odcizení či ztráta, připadají v úvahu pouze u platebních prostředků hmotných, zejména platebních karet.

Podle § 116 odst. 1 písm. b) zákona platebním styku *„[p]látce nese ztrátu z neautorizovaných platebních transakcí v plném rozsahu, pokud tuto ztrátu způsobil svým podvodným jednáním nebo tím, že úmyslně nebo z hrubé nedbalosti porušil některou ze svých povinností stanovených v § 101“*.

To však neplatí v případech, kdy ztrátu z neautorizovaných platebních transakcí nese v plném rozsahu poskytovatel platebních služeb plátce podle § 116 odst. 2 zákona o platebním styku. Jedná se o případy, *„pokud plátce nejednal podvodně a a) ztráta vznikla po té, co plátce oznámil ztrátu, odcizení nebo zneužití platebního prostředku, nebo b) poskytovatel nezajistil, aby uživateli byly k dispozici vhodné prostředky umožňující kdykoliv oznámit ztrátu, odcizení, zneužití nebo neautorizované použití platebního prostředku.“*

Finanční arbitr vychází ze shromážděných podkladů a doložených tvrzení stran sporu, tedy že

(i) platební příkaz ke Sporné platební transakci byl zadán dne 16. 7. 2014 v 15:27:29 hod. a v 15:29:36 hod. potvrzen zadáním autorizačního sms kódu;
(ii) Instituce Spornou platební transakci provedla v 15:29:41 hod;
(iii) Navrhovatel v 15:29:07 hod. kontaktoval telefonicky Instituci; Instituce v telefonickém hovoru Navrhovatele nejprve identifikovala, identifikace skončila po 38 vteřinách od začátku hovoru, tedy v 15:29:45 hod. a Navrhovatel poté označil Spornou platební transakci za neautorizovanou,

a uzavírá, že Navrhovatel oznámil zneužití internetového bankovnictví až po provedení Sporné platební transakce.

Finanční arbitr nemůže přisvědčit námitce Navrhovatele, že ho Instituce ujistila, že Spornou platební transakci neprovede, neboť z obsahu celého telefonického hovoru ze dne 16. 7. 2015, 15:29:07 hod., je zřejmé, že věty citované Navrhovatelem (*„ono by to samozřejmě neodešlo, jo, ono se tam jakoby do mínusu na tom účtu nedostanete, ale už jsem vám to tady nastavil, takže to už ani autorizovat nepůjde“; „teďka máte zablokovaný ten internetbanking, aby vám nemohly být odeslány žádné platby“; a „určitě, právě proto máme tu smsku, aby to tímto způsobem nešlo, pokud by někdo věděl vaše uživatelské jméno a heslo, obejít, jo“*) se netýkají Sporné platební transakce, ale dalších potenciálně zadaných neautorizovaných transakcí

Finanční arbitr naopak Navrhovateli přisvědčuje, že ho Instituce následně skutečně nesprávně informovala o tom, že peněžní prostředky ze Sporné platební transakce nepřipíše na Cílový účet, tak totiž vyplývá ze záznamu telefonního hovoru s názvem „[redacted](Navrhovatelem citované věty *„dobře, já jsem nechala pozastavit všechny platby“; „peníze z účtu odešly, ale jejich odeslání je zastavené; rozhodně nebudou odeslané na ten cílový účet“* a *„nemusíte se bát, ta platba je zablokovaná“*).

Finanční arbitr nemůže než uzavřít, že ztráta ze Sporné platební transakce Navrhovateli vznikla předtím, než plátce (tedy Navrhovatel) oznámil zneužití internetového bankovnictví.

Z poskytnutí nesprávné informace může vyplývat odpovědnost za škodu podle § 2950 občanského zákoníku, který stanoví, že *„[k]do se hlásí jako příslušník určitého stavu nebo povolání k odbornému výkonu nebo jinak vystupuje jako odborník, nahradí škodu, způsobí-li ji neúplnou nebo nesprávnou informací nebo škodlivou radou danou za odměnu v záležitosti svého vědění nebo dovednosti. Jinak se hradí jen škoda, kterou někdo informací nebo radou způsobil vědomě.“* V tomto případě však Instituce škodu takto podanou informací nezpůsobila, neboť peněžní prostředky byly v době poskytnutí informace již připsány na Cílovém účtu a poskytnutí informace na jejich připsání nemělo vliv.

Prostředkem umožňujícím oznámit zneužití internetového bankovnictví je podle čl. XVIa. „Oznámení o zneužití internetbankingu“ odst. 2. Podmínek elektronického bankovnictví telefonní linka Instituce s telefonním číslem [redacted]. Přestože z otisku obrazovky informačního systému Instituce se zobrazením informace o datu a čase začátku a konce telefonického hovoru mezi Navrhovatelem a Institucí ze dne 16. 7. 2015, od 15:29 hod. vyplývá, že Navrhovatel k oznámení zneužití internetového bankovnictví využil linku [redacted], z vyjádření obou stran sporu ani z podkladů shromážděných finančním arbitrem nevyplynulo, že by linka s telefonním číslem [redacted] nebyla v rozhodné době pro tento případ v provozu nebo že by se Navrhovatel pokoušel kontaktovat Instituci na lince [redacted] a nepodařilo se mu to.

Použití ustanovení § 116 odst. 2 zákona o platebním styku tedy v projednávaném případě nepřichází v úvahu a finanční arbitr bude posuzovat odpovědnost za ztrátu ze Sporné platební transakce podle § 116 odst. 1 zákona o platebním styku.

Ze shromážděných podkladů vyplývá, že Sporná platební transakce byla provedena s použitím uživatelského jména a hesla do internetového bankovnictví Navrhovatele a autorizačního sms kódu ke Sporné platební transakci.

Heslo do internetového bankovnictví a autorizační sms kód jsou personalizované bezpečnostní prvky ve smyslu § 85, § 101, § 102 a § 116 zákona o platebním styku, neboť se jimi Navrhovatel musí identifikovat, aby mohl internetové bankovnictví použít k provádění platebních transakcí, a současně nejsou známy třetím osobám.

Podle čl. II. „Způsob přenosu a zabezpečení přenášených dat“ odst. 4 Podmínek elektronického bankovnictví *„[b]anka zřizuje klientovi přístup na neveřejné stránky serveru banky pomocí uživatelského jména a hesla, které si klient zvolí a dohodnutým způsobem předá bance. Klient je oprávněn heslo kdykoliv změnit.“* Podle čl. III. „Autorizace elektronicky podaných pokynů“, odst. 3. Podmínek elektronického bankovnictví *„[a]utorizaci pokynu prostřednictvím sms kódu provádí klient uvedením zaslaného sms kódu do příslušného pole formuláře pro zadávání pokynů v rámci internetbankingu poté, co se řádně přihlásil do internetbankingu svým přihlašovacím jménem a přístupovým heslem. Je-li klientem vložený sms kód shodný s sms kódem vygenerovaným a zaslaným bankou, je pokyn autorizován.“*

Podle § 102 odst. 1 písm. a) zákona o platebním styku *„[p]oskytovatel, který vydává platební prostředek, je povinen zajistit, aby personalizované bezpečnostní prvky platebního prostředku nebyly přístupné osobám jiným než jeho držiteli; tím nejsou dotčeny povinnosti držitele platebního prostředku stanovené v § 101“*.

Jednatel Navrhovatele, který za Navrhovatele vstupoval do internetového bankovnictví Navrhovatele, si zvolil uživatelské jméno a heslo pro první přihlášení ve Smlouvě o elektronickém bankovnictví s Jednatelem Navrhovatele. Tato smlouva současně ve svém čl. II. odst. 3. stanoví, že Jednatel Navrhovatele je povinen při prvním přihlášení k aplikaci

elektronické správy účtů změnit heslo pro přístup k aplikaci elektronické správy účtů, které si zvolil při podpisu smlouvy. Z přihlašovacích údajů do internetového bankovnictví tak lze za personalizovaný bezpečnostní prvek platebního prostředku považovat pouze heslo, nikoliv uživatelské jméno, neboť uživatelské jméno jako údaj uvedený ve smlouvě nebylo známo pouze Jednateli Navrhovatele. Dále je potřeba za personalizovaný bezpečnostní prvek internetového bankovnictví považovat autorizační sms kód, neboť ten Instituce Navrhovateli doručovala na Mobilní telefon Navrhovatele a neměl tak z povahy věci být znám jiným osobám.

Ze shromážděných podkladů finanční arbitr nezjistil, že by splnění povinnost podle § 102 odst. 1 písm. a) zákona o platebním styku Instituce nezajistila. Zjištění finančního arbitra současně nepotvrdila tvrzení Navrhovatele, že se nějakým způsobem lze vyhnout sms autorizaci. Navrhovatel své tvrzení ani nijak nedoložil. Sporná platební transakce proběhla včetně sms autorizace, nikoli bez ní.

Ze shromážděných podkladů má finanční arbitr za to, že ke zneužití internetového bankovnictví Navrhovatele muselo dojít ve sféře Navrhovatele, a to napadením elektronických zařízení, na kterých Navrhovatel používal internetové bankovnictví. Finanční arbitr tak usoudil z tvrzení Navrhovatele, že otevřel přílohu E-mailu od exekutora na svém počítači a nainstaloval do svého mobilního telefonu aplikaci, ve které následně zadal přihlašovací údaje do svého internetového bankovnictví. Personalizované bezpečnostní prvky internetového bankovnictví znal totiž jen Navrhovatel, který, jak sám v Podání vysvětlení PČR tvrdí, že *„[j]á jsem nikomu dalšímu než v tomto popsaném případě nepředával žádné mé přihlašovací údaje. Nikomu jsem ani nepřeposílal ten potvrzovací kód na provedení platby“*.

Podle § 101 písm. a) zákona o platebním styku *„[u]živatel oprávněný používat platební prostředek je povinen používat platební prostředek v souladu s rámcovou smlouvou, zejména je povinen okamžitě poté, co obdrží platební prostředek, přijmout veškerá přiměřená opatření na ochranu jeho personalizovaných bezpečnostních prvků“*.

Ze shromážděných podkladů vyplývá, že pokud Navrhovatel tvrdí, že Spornou platební transakci nezadal, resp. platbu a její potvrzení nezadal, pak tak musela učinit třetí osoba, která ale musela znát heslo do aplikace internetového bankovnictví Navrhovatele i autorizační sms kód.

Finanční arbitr vedl v řízení s obdobným předmětem sporu, ve kterých posuzoval nebo posuzuje stejný typ útoku na internetové bankovnictví. V jednom z posuzovaných případů se jednalo o útok provedený ve stejný den jako v případě Navrhovatele, a současně uživatel internetového bankovnictví taktéž obdržel e-mail, který byl označen jako e-mail od exekutora, a výzvu k instalaci aplikace do svého mobilního telefonu, jde tedy s vysokou mírou pravděpodobnosti o stejný typ útoku. Z Usnesení Policie z jiného sporu vyplývá, že *„neznámý pachatel prostřednictvím tzv. phishingového útoku zaslal oznamovateli e-mail s nepravdivou informací o exekuci, kdy přílohu tohoto e-mailu tvořil archivní soubor s obsahem dalšího spustitelného souboru, který se navenek tvářil jako textový dokument, a po spuštění tohoto souboru, který obsahoval zjevně nesmyslná data, došlo k infikování počítače* [uživatele internetového bankovnictví] *škodlivým software, tzv. virem. Z dosud provedených prověřování týkajících se této vlny phishingových útoků je pak zjednodušeně možno uvést, že škodlivý software, který byl v počítači spuštěn, stáhl další soubory, jejichž účelem bylo monitorovat aktivitu uživatele, zablokovat antivirovou ochranu, zjistit a odeslat informace o internetovém bankovnictví a snaha přesvědčit uživatele nainstalovat si do „chytrého“ telefonu aplikaci, která získala přístup k datům v tomto telefonu, aby bylo možné autorizovat neoprávněné převody z bankovního účtu poškozeného. Po té, co byly všechny podmínky splněny, získal neznámý pachatel přístup k účtu* [uživatele internetového bankovnictví] *a provedl neoprávněný převod finančních prostředků.*

Podle § 85 písm. a) bodu 1. zákona o platebním styku poskytovatel platebních služeb musí uživateli v souladu s § 80 odst. 1 zákona o platebním styku poskytnout informace o povinnostech

a o odpovědnosti poskytovatele a uživatele, mimo jiné, pokud má být podle rámcové smlouvy vydán uživateli platební prostředek, *„popis opatření, která musí uživatel přijmout na ochranu jeho personalizovaných bezpečnostních prvků“*.

V tomto případě tak Instituce učinila ve Smlouvě o elektronickém bankovnictví, resp. v Podmínkách elektronického bankovnictví, a jejím podpisem na sebe Navrhovatel převzal smluvní povinnosti, jejichž účelem je zejména ochrana personalizovaných bezpečnostních prvků internetového bankovnictví, zejména:

1. podle čl. II. „Způsob přenosu a zabezpečení přenášených dat“ odst. 2 Podmínek elektronického bankovnictví: *„Klient je při každém svém připojení na server banky povinen ověřit jeho identifikaci (SHA1 Fingerprint) porovnáním s touto správnou identifikací: D2:31:FA:DA:0D:78:E0:73:31:C4:1C:E7:AB:89:64:9E:25:46:40:E6 (v Microsoft Internet Exploreru je toto číslo zobrazováno bez oddělujících dvojteček). Banka neodpovídá za škodu způsobenou porušením této povinnosti klientem. Identifikaci serveru banky ověříte v okně, které otevřete kliknutím na „žlutou ikonu visacího zámku“, která je umístěna na stránce pro přihlášení do internetbankingu. Tato ikona bývá umístěna obvykle např. na horní nebo dolní ovládací liště v závislosti na použitém webovém prohlížeči. V případě aplikace smartbanking je klient povinen ověřit identitu poskytovatele a autora aplikace při její instalaci do mobilního zařízení, při připojení na server banky prostřednictvím aplikace smartbanking již klient ověření identifikace serveru banky neprovádí.“;*

2. podle čl. VIII. „Pokyny a informace, které lze podávat, resp. získávat prostřednictvím el. správy účtů“ odst. 1 Podmínek elektronického bankovnictví: *„Prostřednictvím elektronické aplikace internetbanking, jež slouží jako komunikační program mezi bankou a klientem, je klient zejména oprávněn zadávat pokyny bance, přijímat od banky informace, zprávy, upozornění, nabídky na platební či bankovní služby, uzavírat s bankou konkrétní smlouvy a i jinak komunikovat s bankou. Z toho důvodu je klient povinen sledovat veškeré zprávy, informace a upozornění, které mu banka prostřednictvím internetbankingu doručí. Neplnění této povinnosti je porušení povinností vyplývajících ze smlouvy.“;*

3. podle čl. XII. „Utajení důvěrných údajů“ odst. 6 Podmínek elektronického bankovnictví: *„Nezasílejte důvěrné údaje pomocí e-mailu nebo sms, nezadávejte je na jiné internetové stránce, než na stránce určené k přihlášení do internetbankingu, a to ani v případě že obdržíte e-mail případně sms, která napodobuje výzvu, zejména od banky, k zaslání důvěrných údajů nebo jejich vyplnění na jiné internetové stránce. Banka Vám takový druh zpráv v žádném případě nebude zasílat.“;*

4. podle čl. XIV. „Preventivní opatření ve sféře vlivu klienta, zabezpečení počítače klienta“ odst. 2 Podmínek elektronického bankovnictví: *„Před přihlášením do internetbankingu se řádně přesvědčte, že komunikujete se správným poskytovatelem služby. Adresa serveru banky je http://www.fio.cz/. Při přihlašování do aplikace internetbanking a při zadávání pokynů prostřednictvím aplikace internetbanking řádně zkontrolujte, že spojení je zabezpečeno (ověřte platnost certifikátu SSL zabezpečení) a dále ověřte identifikaci serveru banky. V případě pochybností o tom, že komunikujete s bankou nebo, že spojení není řádně zabezpečeno, neprovádějte žádné úkony, které by mohly vést k prozrazení nebo zneužití důvěrných údajů a bezodkladně kontaktujte klientského pracovníka banky.“;*

5. podle čl. XIV. „Preventivní opatření ve sféře vlivu klienta, zabezpečení počítače klienta“ odst. 3 Podmínek elektronického bankovnictví: *„Počítač (případně mobilní zařízení jako např. tablet či tzv. chytrý telefon), na kterém se rozhodnete používat internetbanking, zabezpečte legálním firewallem, antivirovou a anti-spyware ochranou, a tyto ochranné*

prvky pravidelně aktualizujte. Programy aktualizujte standardním způsobem. Pravidelně sledujte informace o nových hrozbách, virech, spyware apod. a v souladu s tím zajistěte ochranu Vašeho počítače.“;

6. podle čl. XIV. „Preventivní opatření ve sféře vlivu klienta, zabezpečení počítače klienta“ odst. 5 Podmínek elektronického bankovnictví: „*Používáte-li internetbanking na určitém počítači, vyvarujte se stahování a instalování programů, které lze volně získat na internetu, u nichž si nejste jisti, zda neobsahují viry nebo spyware, případně nepocházejí ze zdroje, který je důvěryhodný. Navštěvujte pouze známé, důvěryhodné a bezpečné stránky na internetu. Neotvírejte nevyžádané emaily, emaily od neznámých adresátů a emaily s podezřelým názvem nebo obsahem na takovém počítači. Takové emaily bez otevření smažte. Ve své emailové schránce používejte spam filtr.“;*

7. podle čl. XIV. „Preventivní opatření ve sféře vlivu klienta, zabezpečení počítače klienta“ odst. 8 Podmínek elektronického bankovnictví: *„Vyspělejší mobilní zařízení (zejména tzv. smartphony a tablety) s operačním systémem iOS, Android, Windows Phone a jiným operačním systémem, je nevyhnutné chránit obdobně jako počítač, a to prostřednictvím legálního antivirového programu; je rovněž žádoucí neinstalovat aplikace z jiných než oficiálních zdrojů pro příslušný operační systém mobilního zařízení (Apple App Store, Google Play, Window Phone Store, atd.).“;*

8. podle čl. XV. „Zabezpečení sms a mobilního zařízení“ odst. 8 Podmínek elektronického bankovnictví: *„I v případě, že na mobilním zařízení nepoužíváte internetbanking ani smartbanking, ale přesto je v takovém mobilním zařízení zapojená SIM karta (tzn. SIM karta, která platí pro telefonní číslo, které je určeno k přijímání autorizačních sms kódů od banky), zabezpečte takové mobilní zařízení legálním firewallem, antivirovou a anti-spyware ochranou a tyto ochranní prvky pravidelně aktualizujte. Programy aktualizujte standardním způsobem. Pravidelně sledujte informace o nových hrozbách, virech, spyware apod. a v souladu s tím zajistěte ochranu Vašeho mobilního zařízení. Postup uvedený v tomto odstavci slouží k omezení rizika utajeného přeposílání autorizačních sms kódů zasílaných bankou (v případě napadeného mobilního zařízení); alternativou k omezení uvedeného rizika je používání SIM karty výlučně v tzv. hloupých telefonech.“*

Podle § 101 písm. a) zákona o platebním styku musí být všechna opatření stanovená rámcovou smlouvou na ochranu personalizovaných bezpečnostních prvků platebního prostředku přiměřená. Přiměřenost je třeba posuzovat s ohledem na konkrétní platební prostředek, v tomto případě internetové bankovnictví. To znamená, že po uživateli platebních služeb nelze požadovat taková opatření, která by výrazně omezovala, případně prakticky znemožňovala používání platebního prostředku.

Finanční arbitr nepovažuje povinnost Navrhovatele stanovenou v čl. II. odst. 2 větě první Podmínek elektronického bankovnictví [tedy povinnost při každém svém připojení na server banky ověřit jeho identifikaci (SHA1 Fingerprint) porovnáním s touto správnou identifikací: D2:31:FA:DA:0D:78:E0:73:31:C4:1C:E7:AB:89:64:9E:25:46:40:E6]**,** v čl. XIV. odst. 2, větě druhé Podmínek elektronického bankovnictví [tedy povinnost při přihlašování do aplikace internetového bankovnictví a při zadávání pokynů prostřednictvím této aplikace řádně zkontrolovat, že spojení je zabezpečeno (tj. ověřit platnost certifikátu SSL zabezpečení) a dále ověřit identifikaci serveru banky] a některé z povinností stanovených v čl. XIV. odst. 5 Podmínek elektronického bankovnictví v jejich obecné formulaci (konkrétně neotvírat nevyžádané emaily a emaily od neznámých adresátů) za přiměřené ve vztahu k ochraně personalizovaných bezpečnostních prvků internetového bankovnictví. Ověřování identifikace serveru Instituce porovnáním s identifikací uvedenou v Podmínkách elektronického bankovnictví

je v prvé řadě Navrhovateli uloženo způsobem, který je podle názoru finančního arbitra pro průměrného uživatele elektronických zařízení těžko pochopitelný (zvláště s přihlédnutím k tomu, že v každém internetovém prohlížeči či i v jednotlivých verzích stejného prohlížeče může být třeba zvolit jiný postup k zobrazení SHA1 Fingerprintu). Nadto, porovnání celkem 40 znaků s identifikací uvedenou ve smlouvě, a to i pouze jednou, je činností poměrně náročnou i pro uživatele s průměrnou pozorovací schopností. Měl-li by tak uživatel internetového bankovnictví činit dokonce při zadávání každého pokynu, pak by plnění takové povinnosti prakticky zcela znemožnilo rozumné používání internetového bankovnictví. V neposlední řadě používají Podmínky elektronického bankovnictví při stanovení těchto povinností odborných výrazů, jejichž význam není průměrnému uživateli znám (SHA1 Fingerprint, SSL zabezpečení), aniž je vysvětlují. Pokud jde o nevyžádané e-maily a e-maily od neznámých adresátů, v tomto případě by důsledné plnění takto obecně formulovaných povinností sice neznemožnilo rozumné používání internetového bankovnictví, znemožnilo by však rozumné používání e-mailové schránky, neboť definici takového e-mailu naplňuje např. každá poptávka od nového klienta v obchodním styku (v tomto případě se jedná jak o nevyžádaný e-mail, tak obvykle i o e-mail od neznámého adresáta). Přiměřenost těchto povinností je proto potřeba posuzovat ve vztahu ke každému konkrétnímu případu.

Za přiměřené finanční arbitr naopak považuje povinnosti uživatele platebního prostředku sjednané mezi Navrhovatelem a Institucí:

1. povinnost vyplývající z § 101 zákona o platebním styku ve spojení s čl. XIV odst. 2 a čl. XII. odst. 6 Podmínek elektronického bankovnictví ověřit adresu serveru banky a přesvědčit se o komunikaci se správným poskytovatelem služby, popř. povinnost nezasílat důvěrné údaje pomocí e-mailu nebo sms, nezadávat je na jiné internetové stránce, než na stránce určené k přihlášení do internetbankingu, a to ani v případě, že uživatel platebních služeb obdrží e-mail případně sms, která napodobuje výzvu, zejména od banky, k zaslání důvěrných údajů nebo jejich vyplnění na jiné internetové stránce;
2. povinnost vyplývající z § 101 zákona o platebním styku ve spojení s čl. XIV. odst. 3 Podmínek elektronického bankovnictví chránit počítač, na kterém uživatel platebních služeb používá internetové bankovnictví (v tomto případě počítač Navrhovatele), antivirovým programem a pravidelně jej aktualizovat, popř. povinnost chránit počítač legálním firewallem;
3. povinnost vyplývající z § 101 zákona o platebním styku ve spojení s čl. XV. odst. 8 Podmínek elektronického bankovnictví chránit mobilní telefon, který uživatel platebních služeb využívá pro přijímání autorizačních sms kódů (v tomto případě Mobilní telefon Navrhovatele), antivirovým programem a pravidelně jej aktualizovat, popř. povinnost chránit Mobilní telefon Navrhovatele legálním firewallem;
4. povinnost vyplývající z § 101 zákona o platebním styku ve spojení s čl. VIII. odst. 1, čl. XIV. odst. 3 a čl. XV. odst. 8 Podmínek elektronického bankovnictví sledovat veškeré zprávy, informace a upozornění, které mu Instituce prostřednictvím internetového bankovnictví doručí;
5. povinnost vyplývající z § 101 zákona o platebním styku ve spojení s čl. XIV odst. 5 Podmínek elektronického bankovnictví vyvarovat se stahování a instalování programů, které lze volně získat na internetu, u nichž není jisté, zda neobsahují viry nebo spyware, případně nepocházejí ze zdroje, který je důvěryhodný, navštěvovat pouze známé, důvěryhodné a bezpečné stránky na internetu, neotevírat nevyžádané e-maily, e-maily od neznámých adresátů (avšak jen s ohledem na okolnosti konkrétního případu) a e-maily s podezřelým názvem nebo obsahem na takovém počítači;
6. povinnost vyplývající z § 101 zákona o platebním styku ve spojení s čl. XIV odst. 8 Podmínek elektronického bankovnictví neinstalovat do chytrého mobilního telefonu

aplikace z jiných než oficiálních zdrojů pro příslušný operační systém mobilního zařízení.

Navrhovatel bude tedy za ztrátu ze Sporné platební transakce odpovídat, pokud ji způsobil svým podvodným jednáním, nebo pokud některou z povinností uvedených v bodech 1. až 6. výše porušil úmyslně anebo z hrubé nedbalosti.

Při vymezení podvodného jednání a jednotlivých forem zavinění, úmyslu a nedbalosti, si soukromé právo vypomáhá právem trestním.

Za podvodné jednání je třeba považovat jednání plátce, kterým úmyslně uvede poskytovatele platebních služeb v omyl anebo jeho omylu využije. Není však třeba, aby zároveň došlo ke spáchání trestného činu podvodu ve smyslu trestního práva.

O úmysl přímý jde tehdy, jestliže osoba, jejíž úmysl se posuzuje, věděla, že svým jednáním může určitý následek způsobit a také ho způsobit chtěla. O úmysl nepřímý jde, jestliže osoba, jejíž úmysl se posuzuje, věděla, že svým jednáním určitý následek způsobit může a je s tímto následkem srozuměna pro případ, že nastane. O nedbalosti vědomé hovoříme tehdy, když osoba, jejíž nedbalost se posuzuje, věděla, že může určitý následek způsobit, ale bez přiměřených důvodů spoléhala, že se tak nestane. O nedbalosti nevědomé hovoříme tehdy, když osoba, jejíž nedbalost se posuzuje, nevěděla, že může určitý následek způsobit, ale vzhledem k okolnostem a k svým osobním poměrům to vědět měla a mohla.

Právní pojem hrubá nedbalost převzal zákon o platebním styku ze Směrnice. Podle úvodního ustanovení Směrnice 33 *„[p]ři posuzování možné nedbalosti na straně uživatele platebních služeb by se mělo přihlédnout ke všem okolnostem. Důkazy a stupeň údajné nedbalosti by se měly hodnotit podle vnitrostátních právních předpisů“.* Pojem hrubé nedbalosti tedy nezávisí na rozlišování nedbalosti vědomé a nevědomé, nedbalost hrubá se tak může vztahovat k oběma stupňům nedbalosti. S pojmem hrubé nedbalosti pracoval zákon č. 40/1964 Sb, občanský zákoník, ve znění pozdějších předpisů (dále jen „zákon č. 40/1964 Sb.“), a to v jediném ustanovení § 447 odst. 2, a od 1. 1. 2014 s ním pracuje občanský zákoník, a to v § 1032 odst. 1, § 2071, § 2072 odst. 1, § 2544, § 2580 odst. 3, § 2898 a § 2971; ani zákon č. 40/1964 Sb. ani občanský zákoník však hrubou nedbalost nedefinuje. Právní pojem hrubá nedbalost vyložily ale obecné soudy. Podle nich se hrubá nedbalost vyznačuje předpokladem zřejmé bezohlednosti (srovnej např. rozhodnutí Nejvyššího soudu ČR ze dne 19. března 1937, Rv I 328/37*: „Hrubá (nápadná) nedbalost jest, jak vyplývá z protikladu lehkého zavinění, neobyčejné zanedbání nutné píle a opatrnosti, které se dopouští jen člověk obzvlášť neopatrný nebo lehkomyslný, který nedbá ani toho stupně opatrnosti, jehož jsou schopni i lidé méně způsobilí než člověk prostředních schopností.“*, rozhodnutí Nejvyššího soudu ČR ze dne 9.10.1924, Rv II 284/24: *„Za hrubou nedbalost lze tedy pokládati jen zvláště těžké porušení povinné bedlivosti, takové, že jeho neblahé následky bylo možno bez námahy předvídati a že se ho bylo možno lehce vyvarovati. Pouhá chyba nebo přehlédnutí, třebas byly spojeny s těžkými následky, mohou se přihoditi i lidem pozorným a pečlivým a nejsou proto samy o sobě důkazem, že vznikly hrubou nedbalostí.“*).

Podle čl. VI „Rozsah odpovědnosti stran“ odst. 3 Podmínek elektronického bankovnictví *„Klient odpovídá za škodu, pokud škodu způsobil svým podvodným jednáním, úmyslně nebo z hrubé nedbalosti. Hrubou nedbalostí se rozumí porušení jakékoli povinnosti klienta vyplývající z článku II, III, IX, X, XII až XIV, XV, XVa, XVI a XVIa Podmínek, zejména porušení opatření za účelem zajištění bezpečnosti a utajení důvěrných údajů, porušení povinností k zabezpečení počítače používaného pro přístup do internetbankingu, porušení povinností k zabezpečení mobilního zařízení/SIM karty používané pro zasílání SMS kódů, porušení povinnosti ověřit identifikaci serveru banky nebo aplikace pro elektronický podpis nebo porušení povinnosti včas oznámit bance podezření na zneužití bezpečnostních údajů.“* Toto vymezení je bez právního

významu, neboť hrubá nedbalost je pojmem právním, a proto obsah tohoto pojmu nemůže být nahrazen dohodou smluvních stran.

Finanční arbitr získal od Instituce Přehled přístupů na WWW, který obsahuje přehled přístupů na webové stránky Instituce z IP adresy [redacted], tedy z IP adresy, ze které se Navrhovatel přihlásil do svého internetového bankovnictví v 12:07:33 hod. a ze které zadal dva platební příkazy, první v 12:14:41 hod. a druhý v 12:16:18 hod.

Přehled přístupů na WWW zaznamenal z IP adresy [redacted]:

a) pohyb na veřejně přístupných webových stránkách Instituce dne 16. 7. 2014 v 12:07:22 hod. a 12:07:23 hod., pohyb na veřejně přístupné webové stránce určené k přihlášení do internetového bankovnictví dne 16. 7. 2014 v 12:07:25 hod. a 12:07:26 hod. (tomu odpovídá tvrzení Navrhovatele *„[p]oužil jsem vyhledávač chrome, kde jsem zadal adresu Fiobanka.cz a otevřela se mi stránky banky. Tam jsem klikl na internetové bankovnictví […]“*);
b) pohyb na zabezpečených webových stránkách Instituce dne 16. 7. 2014 v 12:07:33 hod. (jedná se o čas přihlášení do internetového bankovnictví, to vyplývá také Z Přehledu přístupů do IB a z Přehledu aktivit v IB), 12:07:34 hod., 12:07:35 hod., 12:12:14 hod., 12:12:18 hod. (jedná se o časy, kdy si Navrhovatel zobrazil zůstatky), 12:12:19 hod., 12:13:15 hod. (jedná se o časy, kdy si Navrhovatel zobrazil pohyby na Účtu), 12:13:16 hod., 12:14:35 hod., 12:14:41 hod., 12:15:09 hod., 12:15:15 hod., 12:16:16 hod., 12:16:18 hod. a 12:17:11 hod (jedná se o časy zadání výše uvedených dvou platebních příkazů, tomu odpovídá tvrzení Navrhovatele *„Poté jsem mohl normálně z počítače vstoupit do elektronického bankovnictví, kde jsem normálně prováděl platby a potřebné věci.“).*

Navrhovatel tvrdí, že *„[…] po zadání mých přihlašovacích údajů se mi přímo na stránce FIO banky otevřela povinná aktualizace zvyšování bezpečnosti pomocí chytrého telefonu. Byl jsem vyzván k výběru operačního systému telefonu, kdy bylo na výběr z 5-ti systémů. Já mám android a proto jsem klikl na kolonku s androidem. Pak chtěla aktualizace mé telefonní číslo, které jsem zadal. Jedná se o číslo uvedené shora* ([redacted] – pozn. finančního arbitra). *Během asi 1 minuty jsem obdržel nějakou odpověď z Fiobanky. Nevím již, zda se jednalo o sms, mms nebo nějaký internetový odkaz. Telefon po mě chtěl stáhnout nějakou aplikaci tvářící se jako od Fio banky. Já jsem tak učinil a aplikace mě vyzvala k zadání mých přihlašovacích údajů do elektronického bankovnictví Fiobanky. Já jsem tak učinil a pak se aplikace ukončila. Poté jsem mohl normálně z počítače vstoupit do elektronického bankovnictví, kde jsem normálně prováděl platby a potřebné věci.“* Navrhovatel tak musel tvrzenou instalaci aplikace učinit v čase od 12:07:35 do 12:12:14 hod.

Pokud by běh událostí po sobě následoval tak, jak Navrhovatel popisuje, tedy pokud byl Navrhovatel před instalací aplikace vyzván k výběru operačního systému mobilního telefonu a k zadání svého telefonního čísla, nemohl se v tomto okamžiku pohybovat na webových stránkách Instituce, neboť v opačném případě by tento pohyb byl zaznamenán v Přehledu přístupů na WWW či v Přehledu aktivit v IB, kde je jako poslední aktivita uvedeno zobrazení zůstatku Účtu v 12:07:35 hod. Navrhovatel by tímto nekomunikoval s Institucí jako správným poskytovatelem služby a porušil by povinnost vyplývající z § 101 zákona o platebním styku ve spojení s čl. XIV. odst. 2 Podmínek elektronického bankovnictví, neboť právě toto ustanovení mu ukládá povinnost ověřit adresu serveru a přesvědčit se, že komunikuje se správným poskytovatelem služby. To ostatně přiznává sám Navrhovatel, když tvrdí, že *„[v]še mi připadlo naprosto shodné s Fiobankou s jejich stránkami. Nevšiml jsem si však pod jakou doménou byla ta aktualizace prováděna.“*

Nadto, Navrhovatel tak porušil povinnost vyplývající z § 101 zákona o platebním styku ve spojení s čl. XII. odst. 6 Podmínek elektronického bankovnictví, která ukládá zadávat personalizované bezpečnostní prvky pouze na webové stránce Instituce určené k přihlášení do internetového bankovnictví, neboť Navrhovatel tvrdí, že *„[…] aplikace mě vyzvala k zadání mých přihlašovacích údajů do elektronického bankovnictví Fiobanky. Já jsem tak učinil a pak se aplikace ukončila.“*

Ad 2) a 3)

Navrhovatel sice v průběhu řízení před finančním arbitrem doplnil své původní tvrzení, že na Mobilní telefon Navrhovatele neinstaloval antivirový program nad rámec standardního softwarového vybavení dodaného výrobcem, tak, že je přesvědčen, že na Mobilním telefonu Navrhovatele antivirový program měl, a to buď ze standardního nastavení či od oddělení IT, které mu telefon konfigurovalo a že operační systém Mobilního telefonu Navrhovatele obsahuje ochranné prvky a Navrhovatel jej pravidelně aktualizoval, svá tvrzení však nikdy nedoložil, navíc doplněné tvrzení předložil až poté, co mu finanční arbitr při podání ústního vysvětlení sdělil, že na základě prozatím shromážděných podkladů a jejich posouzení s největší pravděpodobností jednal hrubě nedbale.

Ze shromážděných podkladů současně nevyplývá, že tím Navrhovatel způsobil ztrátu ze Sporné platební transakce. Jak správně upozorňuje Navrhovatel, ani nainstalovaný a řádně aktualizovaný antivirový program nemusí vždy zabránit průniku škodlivého software do příslušného zařízení, zejména z toho důvodu, že autoři antivirových programů logicky aktualizují své virové databáze až po objevení nového viru, přičemž k proniknutí viru do elektronického zařízení může dojít před takovou aktualizací.

Tím, že ale Navrhovatel nepředložil E-mail od exekutora v elektronické podobě, ani svůj Mobilní telefon, se finančnímu arbitrovi nepodařilo zjistit, o jaký konkrétní škodlivý software v tomto případě šlo, ani zda by jeho proniknutí do Mobilního telefonu Navrhovatele jakýkoliv instalovaný antivirový program zabránil. Tím, že Navrhovatel antivirový program do Mobilního telefonu Navrhovatele neinstaloval, riziko proniknutí škodlivého software do Mobilního telefonu Navrhovatele zvýšil.

Navrhovatel označuje ustanovení čl. XIV. Podmínek pro elektronickou správu účtu za příliš vágní, aby mohlo založit povinnosti Navrhovatele, neboť v něm nejsou stanoveny Institucí schválené konkrétní doporučené verze ochranných programů.

Finanční arbitr naopak vzhledem k výše uvedenému považuje toto ustanovení za dostatečně určité, aby založilo povinnost Navrhovatele nainstalovat jakýkoliv antivirový program. Pokud by totiž uživatel platebních služeb učinil a antivirový program pravidelně aktualizoval, nemohl by odpovídat za ztrátu z případné neautorizované platební transakce pro porušení tohoto ujednání, i kdyby k průniku škodlivého software na jeho zařízení došlo.

Pokud jde o legální firewall ochranu, jde o ochranu zpravidla integrovanou v operačním systému a internetových prohlížečích. Uživatel elektronických zařízení tedy v takovém případě nebude muset firewall aktivně instalovat. Uživatel internetového bankovnictví by však neměl firewall vypínat či omezovat jeho funkce. Finanční arbitr v tomto případě neshromáždil žádné podklady, ze kterých by vyplývalo, že tak Navrhovatel učinil, ani to žádná ze stran netvrdí.

Ad 4)

Sledování aktuálních virových hrozeb, které uživateli elektronických zařízení doručuje jeho poskytovatel platebních služeb, považuje finanční arbitr za obezřetné chování průměrného uživatele elektronických zařízení.

Finanční arbitr v řízení zjistil, že Navrhovatel nevěnoval pozornost žádnému z bezpečnostních upozornění, které mu do internetového bankovnictví zaslala Instituce, neboť si žádné z těchto bezpečnostních upozornění ani neotevřel. To vyplývá z bezpečnostních upozornění, která Instituce zaslala do internetového bankovnictví Navrhovatele od 28. 1. 2014 do 18. 7. 2014, ve spojení s otisky informačního systému Instituce se zobrazením informace o přečtení bezpečnostních upozornění a 5 výstupy z informačního systému Instituce se zobrazením záznamů o bezpečnostních upozorněních, která Instituce zaslala do internetového bankovnictví Navrhovatele.

Finanční arbitr nesouhlasí s Navrhovatelem, pokud tvrdí, že mu Instituce tato bezpečnostní upozornění měla zasílat e-mailem. Navrhovatel se Institucí v čl. VIII. odst. 1 Podmínek elektronického bankovnictví výslovně dohodl, že si je bude vyzvedávat právě v internetovém bankovnictví.

Finanční arbitr zjistil, že Instituce Navrhovateli v období od 28. 1. 2014 do 16. 7. 2014 zaslala celkem 6 bezpečnostních upozornění, a to ve dnech 28. 1. 2014, 7. 3. 2014, 11. 3. 2014, 9. 5. 2014, 5. 6. 2014 a 23. 6. 2014. Bezpečnostní upozornění z 28. 1. 2014 mu v internetovém bankovnictví zobrazovala do 28. 5. 2014 (tedy po dobu 4 měsíců), ostatní bezpečnostní upozornění mu zobrazovala minimálně do dne 11. 2. 2015, kdy je finančnímu arbitrovi předložila.

Dne 28. 1. 2014 Instituce zaslala Navrhovateli varování tohoto znění: *„Vážení klienti,
 jelikož v těchto dnech opětovně nabrala na aktuálnosti hrozba tzv. phishingového útoku na účty klientů bank působících v České republice, dovolujeme si vám s měsíčním odstupem od rozeslání poslední výstrahy připomenout důležité zásady bezpečnosti v prostředí internetu, abyste se právě vy oběťmi takového útoku nestali.
 Veškerá elektronická zařízení, na nichž provozujete aplikace Internetbanking a Smartbanking, mějte trvale chráněna účinným a pravidelně aktualizovaným antivirovým programem. Virus označovaný jako "Hesperbot.D", jenž v současné době představuje největší hrozbu, je již velmi dobře prozkoumaný a vhodný antivirový program jej dokáže zavčasu identifikovat a zabránit jeho vniknutí na Váš počítač, tablet či smartphone. Dovolujeme si v této souvislosti zdůraznit, že antivirovým programem je potřeba chránit nejen počítač, ale i tablet či chytrý telefon. I ty se mohou velmi snadno stát místem, kam virus či jiný škodlivý software pronikne a právě dnes nejvíce hrozící útok cílí mimo jiné na ovládnutí mobilních telefonů klientů bank, aby pro pachatele získal autorizační SMS k potvrzení převodních příkazů zadaných na napadených účtech.
 Neotvírejte přílohy e-mailů, jež pocházejí od neznámých adresátů, případně jež na první pohled nejsou určeny právě vám. Stejně tak neprovádějte instalaci žádných aplikací, jejichž účel vám není známý a k jejichž instalaci jste byli vyzváni po kliknutí na určitý odkaz v obdrženém e-mailu. Momentálně nejvíce hrozící virus se šíří e-mailem, který budí dojem oznámení České pošty o nedoručení zásilky a který nabízí možnost získání podrobnějších informací o ní. Pod tímto odkazem je však ukryta výzva k instalaci aplikace, jež je ve skutečnosti škodlivým software (tzv. malware) cílícím na ovládnutí elektronického bankovnictví oběti útoku.
 Na vašem chytrém telefonu, tabletu či jiném obdobném zařízení instalujte jen ty aplikace, které považujete za důvěryhodné a jsou umístěny v oficiálních, kontrolovaných úložištích, např. Google Play pro přístroje s platformou Android či AppStore pro přístroje s platformou iOS. Fio banka, a.s. na vaše mobilní zařízení nezasílá a ani v budoucnu nebude zasílat žádnou výzvu, abyste si zde nainstalovali jakoukoliv aplikaci. Pokud jste si již dříve z vlastního rozhodnutí nainstalovali aplikaci Smartbanking a Fio banka, a.s. přistoupila k jejímu vylepšení, vyzve vás váš přístroj k provedení aktualizace, nikoliv k instalaci nového software. Jakoukoliv výzvu jménem Fio banky k instalaci nového software považujte za podvodnou a obratem nás o tom, prosím, informujte.
 Věříme, že tyto informace jsou pro Vás užitečné a poslouží k co největší míře zabezpečení vašich prostředků na účtech. Všem klientům, kterým jsou výše uvedené zásady bezpečnosti dobře známé, se omlouváme za zbytečnou zprávu, nicméně jsme přesvědčeni, že právě důsledná osvěta a publicita tohoto tématu mezi*

uživateli internetu je v konečném důsledku tím nejlepším prostředkem obrany před elektronickou kriminalitou.“

Dne 9. 5. 2014 Instituce zaslala Navrhovateli varování tohoto znění: *„Vážení klienti, opětovně vás musíme varovat před hrozbou zneužití přístupových údajů do elektronického bankovnictví. Zaznamenali jsme nový typ hrozby útoku na vaše přístupové údaje, který jednoduše poznáte podle existence nového pole "Mobilní telefon" v přihlašovacím formuláři k Internetbankingu - nalézt <A HREF=" http://www.fio.cz/docs/cz/porovnani_praveho_a_falesneho_prihlaseni_do_Fio_Internetbanking.pdf" target="_blank">ZDE</A> Pokud přihlašovací formulář vyžaduje číslo vašeho mobilního telefonu, jste ve skutečnosti na podvodných internetových stránkách a s velkou pravděpodobností je Váš počítač napaden škodlivým software, případně byl napaden Váš domácí router. V případě, že se s takto podvrženou přístupovou stránkou setkáte, v žádném případě nezadávejte vaše přístupové údaje, s vysokou mírou pravděpodobnosti se bude jednat o pokus o elektronický útok. Pokud jste se dosud na takto napadeném počítači nepřihlásili, podnikněte kroky k jeho odvirování. Pokud jste již své přístupové údaje do takového formuláře zadali, nastavte si nové heslo z jiného, nenapadeného počítače. Pokud nemáte možnost přenastavit heslo z nenapadeného PC, kontaktujte nás na pobočce. V čase mimo provozní hodiny pobočky, nás kontaktujte na lince pro hlášení ztráty/krádeže karty vydané Fio bankou:* [redacted] *Pro obecné zásady bezpečnosti, Fio banka doporučuje používat DNS server se schopnostmi DNSSEC, aktualizovaný software počítače, ale také zabezpečený domácí router, atd. Váš tým klientské podpory“*

Byť se ani jedno z citovaných varování nevztahuje na konkrétní případ, se kterým se setkal Navrhovatel, dává varování ze dne 28. 1. 2014 pokyny, jimiž se Navrhovatel v tomto případě neřídil. Jedná se konkrétně o pokyn, aby uživatel chránil nejen počítač, ale i svůj mobilní telefon, prostřednictvím kterého přijímá autorizační sms, antivirovým programem a pravidelně jej aktualizoval, aby neotevíral přílohy e-mailů, jež pocházejí od neznámých adresátů, případně jež na první pohled nejsou určeny právě jemu [Navrhovatel přesto otevřel přílohu e-mailové zprávy, o které věděl, že není určena jemu (neboť sám tvrdí, že se domníval, že jde o e-mail adresovaný [redacted] a aby na svůj chytrý telefon instaloval jen ty aplikace, které považuje za důvěryhodné a jsou umístěny v oficiálních, kontrolovaných úložištích, např. Google Play pro přístroje s platformou Android, neboť Instituce na mobilní zařízení uživatelů nezasílá a ani v budoucnu nebude zasílat žádnou výzvu, aby si zde nainstalovali jakoukoliv aplikaci (Navrhovatel přesto uposlechnul výzvy, aby si do svého mobilního telefonu nainstaloval „bezpečnostní aplikaci“ a učinil tak i přesto, že nebyla umístěna na oficiálním kontrolovaném úložišti pro přístroje s platformou Android, v tomto případě Google Play). I u Smartbankingu, pokud by jej měl uživatel nainstalovaný, vyzve mobilní telefon uživatele k provedení aktualizace, nikoliv k instalaci nového software. Jakoukoliv výzvu jménem Instituce k instalaci nového software měl uživatel považovat za podvodnou.

Jedná se obecné bezpečnostní zásady, které, byť odeslány dne 28. 1. 2014, neztratily nic na své aktuálnosti ani ke dni provedení Sporné platební transakce. Argument Navrhovatele, že v době provedení Sporné platební transakce bylo varování ze dne 28. 1. 2014 zcela neaktuální s ohledem na dynamický vývoj počítačového pirátství, tak v tomto případě neobstojí. Své tvrzení Navrhovatel opět ničím nedokládá.

Pokud jde o varování z 9. 5. 2014, má sice finanční arbitr za to, že i z něho mohl Navrhovatel čerpat určité podněty, které by mu pomohly vyvarovat se napadení jeho mobilního telefonu *(„[p]okud přihlašovací formulář vyžaduje číslo vašeho mobilního telefonu, jste ve skutečnosti na podvodných internetových stránkách a s velkou pravděpodobností je Váš počítač napaden škodlivým software, případně byl napaden Váš domácí router“)*, přesto však jde o varování před konkrétním a v podrobnostech odlišným typem útoku, proto k tomuto varování finanční arbitr nepřihlédl.

Navrhovatel namítá, že konkrétní varování před útokem, jehož obětí se Navrhovatel stal při provedení Sporné platební transakce, Instituce zaslala až dne 18. 7. 2014, tedy po provedení Sporné platební transakce. Tomu finanční arbitr přisvědčuje, ale znovu opakuje, že již varování ze dne 28. 1. 2014 obsahovalo dostatek informací a pokynů, při jejichž dodržení by Navrhovatel provedení Sporné platební transakce s největší pravděpodobností zabránil.

Finanční arbitr uzavírá, Navrhovatel porušil smluvně převzatou povinnost sledovat veškeré zprávy, informace a upozornění, které mu Instituce prostřednictvím internetového bankovnictví doručí.

Ad 5)

Pokud jde o E-mail od exekutora, musí jej finanční arbitr posuzovat s ohledem na povinnost stanovenou Navrhovateli v čl. XIV., odst. 5 Podmínek elektronického bankovnictví, tj. neotvírat nevyžádané e-maily, e-maily od neznámých adresátů a e-maily s podezřelým názvem nebo obsahem na počítači, na kterém používá internetové bankovnictví. Finanční arbitr má za to, že tento e-mail průměrnému uživateli sám o sobě nemusel připadat podezřelý. Přestože soudní exekutor zásadně podobné výzvy prostřednictvím e-mailové pošty nezasílá, nemůže průměrný uživatel při obdržení podobného e-mailu jednoznačně určit, že soudní exekutor nemohl takový e-mail poslat, byť to zákon č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) a o změně dalších zákonů, ve znění pozdějších předpisů, nepředpokládá. Průměrný uživatel mohl sice dospět k závěru, že zasláním takového e-mailu soudní exekutor překračuje zákon a že pro něho tudíž takový e-mail není relevantní, nikoliv však k závěru, že musí jít o podvodný e-mail, a zejména nikoliv k závěru, že by mohl mít spojitost s používáním internetového bankovnictví. Navrhovatel však sám tvrdí, že tento e-mail nebyl určen jemu a jedná se tedy o nevyžádaný e-mail. Vzhledem k jeho obsahu se Navrhovatel nemohl ani domnívat, že je e-mail, přestože byl zaslán na cizí e-mailovou adresu, určen jemu. Navrhovatel tak minimálně neměl otevírat přílohu tohoto e-mailu. Navrhovatel tím proto porušil povinnost stanovenou v čl. XIV., odst. 5 Podmínek elektronického bankovnictví.

Ad 6)

Navrhovatel neupřesňuje, jakým způsobem obdržel výzvu k instalaci „bezpečnostní aplikace“ na Mobilní telefon Navrhovatele, resp. v podrobnostech se jeho tvrzení liší (jednou ji označuje za výzvu k nainstalování aplikace na svůj mobilní telefon, jednou za výzvu k aktualizaci programu vydaného Institucí).

Finanční arbitr má za to, že se tak stalo prostřednictvím odkazu obsaženého v sms zprávě doručené na Mobilní telefon Navrhovatele, neboť Navrhovatel podle svého tvrzení k výzvě zobrazené na počítači zadal číslo svého mobilního telefonu. Žádal-li útočník právě o číslo mobilního telefonu, musel výzvu k instalaci „bezpečnostní aplikace“ zaslat právě prostřednictvím sms zprávy, neboť při znalosti právě jen telefonního čísla nelze odkaz zaslat jiným kanálem (např. e-mailem, prostřednictvím facebooku nebo chatovací služby).

Finanční arbitr vylučuje, že by mohlo jít o aplikaci pocházející z oficiálního úložiště pro Android – Google Play, neboť je finančnímu arbitrovi známo a Navrhovatel sám zdůrazňuje, že aplikace dostupné na tomto úložišti jsou prověřené. Proto se muselo jednat o aplikaci, kterou si Navrhovatel stáhnul z jiného zdroje. Tento závěr podporují zjištění finančního arbitra v řízeních s obdobným předmětem sporu, ve kterých finanční arbitr posuzoval stejný typ elektronického útoku, neboť v těchto případech na mobilní telefon uživatele přišla sms s odkazem na stažení aplikace. V jednom z posuzovaných případů se dokonce jednalo o útok provedený ve stejný den jako v případě Navrhovatele, a současně uživatel internetového bankovnictví taktéž obdržel e-mail, který byl označen jako e-mail od exekutora, jde tedy s vysokou mírou pravděpodobnosti

o stejný typ útoku. V tomto případě uživatel internetového bankovnictví obdržel sms s odkazem bit.ly/1IEMJUN. To vyplývá z Usnesení Policie z jiného sporu.

Finanční arbitr měl původně v úmyslu provést ohledání Mobilního telefonu Navrhovatele. Ten jej však finančnímu arbitrovi nepředložil, proto finanční arbitr provedl zkoumání telefonu stejné značky, typu a se stejným operačním systémem, tj. mobilní telefon Samsung Galaxy S5 Black, sériové číslo [redacted] s operačním systémem Android ve verzi standardně s tímto typem přístroje výrobcem dodávané (dále jen „Testovací telefon“).

Navrhovatel ani nesdělil finančnímu arbitrovi přesnou verzi operačního systému Android, finanční arbitr však nezjistil, že by případné rozdíly mezi jednotlivými verzemi mohly mít v tomto případě zásadní vliv na chování a ovládání telefonu co do průběhu instalace nových aplikací (podle tvrzení Instituce je určitý typ telefonu standardně výrobcem dodáván s jednou určitou verzí operačního systému; uživatel si může tuto verzi průběžně aktualizovat, finanční arbitr však má za to, že v případných novějších verzích nebude uživateli k dispozici méně bezpečnostních hlášení než v základní verzi, spíše tomu bude naopak).

Finanční arbitr zkoumáním Testovacího telefonu zjistil, že tento telefon je z výroby nastaven tak, že na něm nelze bez dalšího provádět instalaci aplikací z jiných zdrojů než z úložiště z Google Play. Současně je telefon nastaven tak, aby „ověřoval aplikace“, tzn. aby uživatele upozornil, že aplikace, kterou se chystá nainstalovat, může potenciálně být škodlivá.

Pokud se uživatel na Testovacím telefonu pokusí otevřít odkaz na jakoukoliv aplikaci, která nepochází z Google Play, Testovací telefon zobrazí upozornění: *„Používáním neznámých odkazů ohrožujete své zařízení a osobní údaje. Klepnutím na tlačítko Ok potvrdíte souhlas s tím, že nesete plnou odpovědnost za jakékoli poškození zařízení nebo ztrátu dat způsobené použitím tohoto odkazu.“* Tento text je doprovázen tlačítky *„Zrušit“* (jako první v řadě) a *„OK“*. Klikne-li uživatel na tlačítko *„OK“*, Testovací telefon nabídne uživateli, jakou aplikací chce akci dokončit (v tomto případě *„Internet“* a *„Chrome“*) a poté, co si uživatel aplikaci vybere a potvrdí, aplikaci na příslušném odkazu stáhne. Na staženou aplikaci pak uživatel klikne a Testovací telefon zobrazí upozornění: *„Aplikace byla zablokována. Z důvodu zabezpečení je zařízení nyní nastaveno tak, že blokuje instalaci aplikací, které nepocházejí z Play Store. Chcete-li to změnit, přejděte na Nastavení > Zabezpečení > Neznámé zdroje.“* Tento text je doprovázen tlačítky *„Zrušit“* (jako první v řadě) a *„Nastavení“*. Klikne-li uživatel na *„Nastavení“*, bude mít možnost v sekci Nastavení / Správa zařízení zakliknout položku Neznámé zdroje. Pokud tak učiní, Telefon zobrazí upozornění: *„Neznámé zdroje. Instalace z neznámých zdrojů může být škodlivá pro vaše zařízení a osobní data. Klepnutím na tlačítko Ok potvrdíte souhlas s tím, že nesete plnou odpovědnost za jakékoli poškození zařízení nebo ztrátu dat způsobené použitím těchto aplikací.“* Tento text je doprovázen zaklikávací položkou *„Povolit pouze tuto instalaci“* (předzaškrtnutou) a tlačítky *„Zrušit“* (jako první v řadě) a *„OK“*. Klikne-li uživatel na tlačítko *„OK“*, Testovací telefon zobrazí text: *„Chcete tuto aplikaci nainstalovat? Aplikace získá přístup k těmto oprávněním:“* a následuje seznam příslušných oprávnění (např. určení polohy, ale záleží na tom, k jakým konkrétním oprávněním právě daná aplikace přístup požaduje; v případě viru, který má za cíl předávání autorizačních sms, by se zřejmě jednalo o přístup k sms zprávám) doprovázený tlačítky *„Zrušit“* (jako první v řadě) a *„Instalovat“*. Klikne-li uživatel na tlačítko *„Instalovat“*, aplikace se nainstaluje.

Finanční arbitr dále zkoumal, jak by instalace z neznámého zdroje probíhala v případě, že by uživatel již dříve změnil výrobní nastavení Testovacího telefonu tak, že by povolil instalaci aplikací z jiných zdrojů než z úložiště z Google Play (přičemž by obdržel shora citované upozornění *„[n]eznámé zdroje. Instalace z neznámých zdrojů může být škodlivá pro vaše zařízení a osobní data. Klepnutím na tlačítko Ok potvrdíte souhlas s tím, že nesete plnou odpovědnost za jakékoli poškození zařízení nebo ztrátu dat způsobené použitím těchto aplikací“*),

popř. současně telefon nastavil tak, aby „neověřoval aplikace“. Finanční arbitr zjistil, že Testovací telefon by i po takové změně zobrazil výše citované upozornění *„[p]oužíváním neznámých odkazů ohrožujete své zařízení a osobní údaje. Klepnutím na tlačítko Ok potvrdíte souhlas s tím, že nesete plnou odpovědnost za jakékoli poškození zařízení nebo ztrátu dat způsobené použitím tohoto odkazu.“* a dále by i po takové změně zobrazil seznam oprávnění, ke kterým daná aplikace požaduje přístup.

S ohledem na výsledky ohledání Testovacího telefonu tak finanční arbitr dospěl k závěru, že Navrhovatel musel při instalaci aplikace do Mobilního telefonu Navrhovatele obdržet a ignorovat shora citovaná upozornění. Navrhovatel instalací této aplikace porušil povinnost stanovenou čl. XIV. odst. 5 Podmínek elektronického bankovnictví neinstalovat aplikace z jiných než oficiálních zdrojů pro příslušný operační systém mobilního zařízení (v tomto případě Google Play).

Jak se vyjádřil i Ústavní soud *„v civilním řízení nemusí nepřímé důkazy tvořit zcela uzavřenou soustavu, která nepřipouští jiný skutkový závěr než ten, k němuž soud dospěl, nýbrž dostačuje, jestliže nepřímé důkazy s velkou mírou pravděpodobnosti k tomuto závěru (na rozdíl od možných závěrů jiných) vedou“* (rozsudek ÚS ze dne 2. 12. 2004, sp. zn. II ÚS 66/03). Obdobně i Nejvyšší soud ve svém rozhodnutí sp. zn. 21 Cdo 2682/2013 ze dne 26. 6. 2014 dospěl k závěru, že *„…skutečnost prokazovanou pouze nepřímými důkazy lze mít za prokázanou, jestliže na základě výsledků hodnocení těchto důkazů lze bez rozumných pochybností nabýt jistoty (přesvědčení) o tom, že se tato skutečnost opravdu stala (že je pravdivá); nestačí, lze-li usuzovat pouze na možnost její pravdivosti (na její pravděpodobnost) …“*

V tomto případě se nepodařilo finančnímu arbitrovi prokázat veškeré konkrétní okolnosti napadení elektronických zařízení Navrhovatele počítačovým virem. Z podkladů, které si finanční arbitr opatřil, a ze zjištění, které finanční arbitr učinil, ve spojení s tvrzeními samotného Navrhovatele, však nepochybuje o tom, že Navrhovatel musel učinit několik po sobě jdoucích kroků, přičemž tyto kroky jednotlivě vedly k napadení elektronických zařízení Navrhovatele (počítače a Mobilního telefonu Navrhovatele) a v souhrnu třetí osobě umožnily úspěšné zadání Sporné platební transakce. Navrhovatel podle finančního arbitra nezajistil ochranu svých elektronických zařízení a tím i personalizovaných bezpečnostních prvků, resp. nepřijal veškerá přiměřená opatření na jejich ochranu.

Finanční arbitr nezjistil, že by Navrhovatel některou ze zákonných nebo smluvně převzatých povinností porušil úmyslně.

V tomto případě je však ze shromážděných podkladů a jejich posouzení zřejmé, že se na straně Navrhovatele nejednalo o ojedinělou chybu či přehlédnutí, ale o neobyčejnou lehkomyslnost, lhostejnost a bezohlednost, kterou projevoval ve vztahu k používání platebního prostředku, kterým je v tomto případě internetové bankovnictví, a k elektronickým zařízením, na kterých tento platební prostředek používal. Navrhovatel porušil nikoli jednu, ale více povinností stanovených Smlouvou o elektronickém bankovnictví, přičemž teprve souhrnné porušení těchto povinností vedlo ke ztrátě ze Sporné platební transakce. Navrhovatel projevil naprostý nezájem o bezpečnostní otázky související s používáním internetového bankovnictví a zcela ignoroval jakékoli bezpečnostní zásady, jejichž cílem je ochrana personalizovaných bezpečnostních prvků.

Navrhovatel si nepřečetl ani jedno z bezpečnostních upozornění, které mu Instituce od uzavření Smlouvy o elektronické správě účtu zaslala (přestože mu je Instituce v internetovém bankovnictví zobrazovala po dobu 4 měsíců, popř. dosud). Finanční arbitr považuje takovou nečinnost Navrhovatele za hrubou nedbalost, neboť projevil naprostý nezájem o bezpečnostní otázky.

Pokud jde o povinnost ověřit adresu serveru a přesvědčit se, zda Navrhovatel komunikoval se správným poskytovatelem služby, Navrhovatel tak neučinil ani v situaci, kdy, jak Navrhovatel tvrdí, nemohl internetové bankovnictví standardním způsobem používat. Podle čl. II. „Způsob přenosu a zabezpečení přenášených dat“ odst. 4 Podmínek elektronického bankovnictví Instituce zřizuje Navrhovateli přístup na neveřejné stránky serveru Instituce (tedy do internetového bankovnictví) pomocí uživatelského jména a hesla. Instituce tak podle Smlouvy o elektronickém bankovnictví musí Navrhovateli zpřístupnit internetové bankovnictví po zadání uživatelského jména a hesla a bez další dohody s Navrhovatelem nemůže k přihlášení požadovat další kroky Navrhovatele. I to, že Instituce odepírá přístup do internetového bankovnictví dohodnutým způsobem, by obezřetný uživatel musel nutně považovat za podezřelé.

V případě instalace aplikace dospěl finanční arbitr k závěru, že Navrhovatel jednal hrubě nedbale, neboť Navrhovatel si musel vzhledem k výše citovaným upozorněním být vědom, že se při práci s elektronickým zařízením nechová bezpečně, a přesto provedl instalaci bez dalšího ověření bezpečnosti aplikace (což by průměrně obezřetný uživatel musel učinit). Nadto tak učinil v přímé vazbě na používání internetového bankovnictví, když reagoval na výzvu obdrženou po přihlášení do internetového bankovnictví. V obezřetném uživateli by musela výše citovaná upozornění nutně vzbudit podezření, že něco není v pořádku, a kontaktoval by svou banku pro ověření, zda mu skutečně zaslala aplikaci, kterou jeho mobilní telefon označuje na nebezpečnou.

V tomto případě byly personalizované bezpečnostní prvky používány výhradně prostřednictvím elektronických zařízení. Ochrana personalizovaných bezpečnostních prvků platebního prostředku zahrnovala nejen povinnost chránit samotné personalizované bezpečnostní prvky, ale také povinnost chránit elektronická zařízení, prostřednictvím kterých platební prostředek používá (v případě Navrhovatele se jednalo o počítač a Mobilní telefon Navrhovatele), popř. vyvarovat se použití platebního prostředku v případech, kdy by uživatel platebních služeb takovou ochranu nemohl zajistit.

9. K ostatním námitkám Navrhovatele

Po provedení Sporné platební transakce již Instituce nemohla peněžní prostředky odebrat z Cílového účtu, neboť by tak sama provedla neautorizovanou platební transakci, za kterou by v takovém případě nesla odpovědnost. Instituce však tím, že Spornou platební transakcí oznámila Ministerstvu financí jako podezřelý obchod, učinila vše, co bylo po ní možné požadovat, aby zabránila, že peněžní prostředky odpovídající částce Sporné platební transakce budou z Cílového účtu vybrány nebo převedeny na jiný účet. Peněžní prostředky odpovídající částce Sporné platební transakce byly poté na Cílovém účtu zajištěny podle § 79a trestní řádu a Navrhovatel jako poškozený se jejich vrácení může domáhat podle § 81a trestního řádu.

Finanční arbitr nemůže přisvědčit Navrhovateli, že by Instituce měla sledovat IP adresy, ze kterých uživatelé zadávají platební příkazy, neboť v případě Navrhovatele byl platební příkaz ke Sporné platební transakci zadán z jiné IP adresy, než ze které se Navrhovatel standardně přihlašuje. Takovou povinnost Instituci žádný právní předpis neukládá, ani si ji s Navrhovatelem nesjednala a z povahy věci neměla bránit svým klientům v používání internetového bankovnictví z různých přístrojů, ani v používání anonymizačních služeb z důvodu ochrany soukromí.

Tvrzení Navrhovatele, že jiní poskytovatelé platebních služeb peněžní prostředky svým uživatelům v obdobných případech vrátili, nelze považovat za důvodnou námitku. Navrhovatel nedoložil, že se jednalo o obdobné případy, ani že tak instituce učinily, protože jim vznikla odpovědnost za neautorizovanou platební transakci ve smyslu § 116 zákona o platebním styku.

Ani Navrhovatelova vyhrůžka medializací celého případu nemůže vést k tomu, aby finanční arbitr rozhodl jinak, než mu ukládá zákon, tedy na základě právního posouzení skutkového stavu věci a volného hodnocení shromážděných podkladů. Finanční arbitr je povinen při řešení sporů postupovat stejně jako obecný soud, nikoli podle představ jedné ze stran sporu.

Námitku Navrhovatele, že v řízení před finančním arbitrem byla porušena zásada nestrannosti, neboť finanční arbitr nařídil ústní jednání v sídle Instituce, finanční arbitr odmítá jako účelovou. Navrhovatel nijak neodůvodnil, jakým způsobem mělo konání ústního jednání v sídle Instituce, k němuž byl sám přizván, zasáhnout do nestrannosti finančního arbitra. Navíc, podle § 12 odst. 6 zákona o finančním arbitrovi je finanční arbitr oprávněn nahlédnout do spisů a elektronických záznamů Instituce; tyto úkony provádí finanční arbitr z povahy věci v sídle Instituce.

A konečně, finanční arbitr nemůže nahlížet do spisu trestního řízení jako zmocněnec Navrhovatele, neboť při výkonu své činnosti musí být nestranný a nesmí činit nic, co by jeho nestrannost mohlo ohrozit nebo zpochybnit (§ 5 zákona o finančním arbitrovi); nemůže tedy působit jako zmocněnec některé ze stran. Navrhovatel jako oznamovatel podezření ze spáchání trestného činu a současně poškozený podle § 43 trestního řádu je osobou oprávněnou nahlížet do spisu trestního řízení podle § 65 trestního řádu.

10. K výroku rozhodnutí

Na základě shromážděných podkladů a jejich posouzení nezjistil finanční arbitr, že by ztrátu ze Sporné platební transakce způsobila Instituce.

Na základě shromážděných podkladů a jejich posouzení dospěl finanční arbitr k závěru, že Navrhovatel nezpůsobil ztrátu ze Sporné platební transakce podvodně nebo úmyslně, ale tím, že z hrubé nedbalosti porušil zákonné a smluvně převzaté povinnosti:

a) povinnost sledovat bezpečnostní upozornění, které mu zasílala Instituce, vyplývající z § 101 zákona o platebním styku ve spojení s čl. VIII. odst. 1, čl. XIV. odst. 3 a čl. XV. odst. 8 Podmínek elektronického bankovnictví,
b) povinnost ověřit adresu serveru a přesvědčit se o správném poskytovateli služby vyplývající z § 101 zákona o platebním styku ve spojení s čl. XIV odst. 2 a čl. XII. odst. 6 Podmínek elektronického bankovnictví,
c) povinnost neinstalovat do chytrého mobilního telefonu aplikace z jiných než oficiálních zdrojů pro příslušný operační systém mobilního zařízení vyplývající z § 101 zákona o platebním styku a čl. XIV. odst. 8 Podmínek elektronického bankovnictví.

Odpovědnost za ztrátu z neautorizovaných platebních transakcí proto nese Navrhovatel podle § 116 odst. 1 písm. b) ve spojení s § 101 odst. a) zákona o platebním styku v plném rozsahu.

Na základě všech výše uvedených skutečností rozhodl finanční arbitr tak, jak je uvedeno ve výroku tohoto rozhodnutí.

P o u č e n í :

Proti tomuto nálezu lze podle § 16 odst. 1 zákona o finančním arbitrovi do 15 dnů od jeho doručení podat písemně odůvodněné námitky k finančnímu arbitrovi. Práva podat námitky se lze vzdát. Včas podané námitky mají odkladný účinek.

Podle § 17 odst. 1 zákona o finančním arbitrovi, nález, který již nelze napadnout námitkami, je v právní moci.

V Praze dne 18. 11. 2015

otisk úředního razítka

Mgr. Monika Nedelková
finanční arbitr