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/583/2016
Spisová značka (uvádějte vždy v korespondenci):
FA/PS/127/2015

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 jen „zákon o finančním arbitrovi“), rozhodl v řízení zahájeném dne 22. 2. 2015 podle § 8 zákona o finančním arbitrovi o návrhu navrhovatele [redacted] (dále jen „Navrhovatel“), proti instituci Fio banka, a.s., IČO 61858374, 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 234.520 Kč, 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

Navrhovatel se po Instituci domáhá vrácení peněžních prostředků ve výši částky platební transakce, kterou Instituce provedla na základě platebního příkazu zadaného z internetového bankovnictví Navrhovatele, ale který Navrhovatel nezadal.

Finanční arbitr při zkoumání podmínek řízení zjistil, že Navrhovatel uzavřel s Institucí dne 5. 4. 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.

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“).

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. I. „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 4. 11. 2013 Navrhovateli změnu podmínek vedení účtů a podmínek elektronického bankovnictví s účinností od 6. 1. 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 6. 1. 2014 (dále též „Podmínky vedení účtů z 6. 1. 2014“) a za součást Smlouvy o elektronickém bankovnictví Podmínky vedení účtů z 6. 1. 2014 a Obchodní podmínky pro elektronickou správu účtů účinné od 6. 1. 2014 (dále jen „Podmínky elektronického bankovnictví z 6. 1. 2014“).

Podmínky vedení účtů z 6. 1. 2014 ve svém čl. I. „Předmět úpravy“, odst. 4 stanoví: *„Banka je oprávněna navrhnout klientovi změnu smlouvy, na základě které provádí klient platební styk (např. smlouva o běžném účtu nebo o účtu 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 navrženou účinností změny smlouvy, a to prostřednictvím internetbankingu, pokud ho má klient zřízený, nebo na jiném trvalém nosiči dat, anebo osobně na pobočce banky, která klientovi vede účet. Platí (smluvní strany se tak dohodly), že klient návrh na změnu smlouvy přijal, jestliže (i) byl návrh poskytnut klientovi způsobem a ve lhůtě podle předchozí věty, (ii) klient návrh na změnu smlouvy neodmítl, (iii) banka o tomto důsledku klienta v návrhu informovala a (iv) banka v návrhu na změnu smlouvy informovala klienta o jeho právu bezúplatně a s okamžitou účinností vypovědět smlouvu přede dnem, kdy má navrhovaná změna nabýt účinnosti, pokud klient takový návrh odmítne. Pokud klient návrh na změnu smlouvy odmítne, má právo smlouvu přede dnem, kdy má změna smlouvy nabýt účinnosti, bezúplatně a s okamžitou účinností vypovědět.“* Stejný způsob změny Podmínek elektronického bankovnictví z 6. 1. 2014 stanoví Podmínky elektronického bankovnictví z 6. 1. 2014 ve svém čl. XVII. „Závěrečná ustanovení“, odst. 1.

Finanční arbitr z přehledu a obsahu zpráv, které Instituce zobrazila Navrhovateli v internetovém bankovnictví, dále zjistil, že Instituce v souladu s § 94 zákona o platebním styku, s čl. I. „Předmět úpravy“, odst. 4 Podmínek vedení účtů z 6. 1. 2014 a s čl. XVII. „Závěrečná ustanovení“, odst. 1. Podmínek elektronického bankovnictví z 6. 1. 2014 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 5. 4. 2013 do 5. 1. 2014 Podmínky vedení účtů z 1. 3. 2013, od 6. 1. 2014 do 1. 6. 2014 Podmínky vedení účtů z 6. 1. 2014 a od 2. 6. 2014 Podmínky vedení účtů. Součástí Smlouvy o elektronickém bankovnictví pak byly od 5. 4. 2013 do 5. 1. 2014 Podmínky elektronického bankovnictví z 18. 6. 2012 a Podmínky vedení účtů z 1. 3. 2013, od 6. 1. 2014 do 1. 6. 2014 Podmínky elektronického bankovnictví z 6. 1. 2014 a Podmínky vedení účtů z 6. 1. 2014 a od 2. 6. 2014 Podmínky elektronického bankovnictví a Podmínky vedení účtů.

Internetové bankovnictví, prostřednictvím kterého Navrhovatel Účet spravoval, je platebním prostředkem ve smyslu § 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 účtu platebního 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 odst. 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 v návrhu na zahájení řízení označuje za předmět sporu *„zneužití aplikace internetového bankovnictví a s tím související podvodné autorizace platby ze dne 16. 7. 2014 osobou, která nebyla oprávněná s účtem nakládat“*.

Navrhovatel tvrdí, že dne 10. 7. 2014 si [redacted], založil u Instituce účet č. [redacted] (dále jen „Cílový účet“), na který byla dne 16. 7. 2014 z Účtu převedena částka 234.520 Kč, variabilní symbol [redacted], zpráva pro příjemce “záloha“. Navrhovatel dále tvrdí, že [redacted] ve stejný den vybral celou částku ve třech pobočkách Instituce, a to v 13.25 hod. částku 100.000 Kč na pobočce na Praze 10, Moskevská, v 14.00 hod. částku 100.000 Kč na pobočce na Praze 1, V Celnici a v 14.45 hod. částku 34.000 Kč na pobočce na Praze 5, Ječná.

Navrhovatel namítá, že podle pravidel týkajících se výběru hotovosti u Instituce zjištěných na její pobočce v Ústí nad Labem je možné v hotovosti na pobočce bez předchozího nahlášení výběru vybrat částku do 50.000 Kč.

Navrhovatel v Protokolu Policie ČR, který učinil součástí návrhu na zahájení řízení před finančním arbitrem, popisuje, že dne 15. 7. 2014 v 23:30 hod. obdržel e-mail od exekutora, který jej vyzval k zaplacení částky 12.000 Kč s odkazem na informace v příloze e-mailu. Navrhovatel tvrdí, že přílohu otevřel, ale protože se objevil nějaký anglický text, usoudil, že se jedná o spam. Navrhovatel dále popisuje, že následně, neví přesně kdy, se *„jako obvykle přihlásil ke svému výše uvedenému bankovnímu účtu, prostřednictvím elektronického bankovnictví za pomoci mého* [tj. Navrhovatelova – pozn. finančního arbitra] *notebooku. Po přihlášení na portál Fio banky jsem byl vyskakovacím oknem vyzván, abych v rámci zvýšení bezpečnosti přístupu na účet stáhl mobilní aplikaci do svého mobilního telefonu, která mi vygeneruje kód pro následné přihlášení do aplikace internetového bankovnictví. Na základě tohoto požadavku, který se tvářil jako požadavek Fio banky jsem si uvedenou aplikaci s názvem Fio Banka OTP Direct stáhl do mobilu. Stalo se to tak, že po potvrzení, že aplikaci chci do mobilu stáhnout, mi na můj mobilní telefon zn. Samsung Xcover se sim kartou s účastnickým číslem: [redacted] přišla SMS zpráva, kdy odesílatel byl: INFO, kdy znění zprávy bylo: Odkaz: [redacted], na tento odkaz jsem kliknul a do mobilu se tak pomocí mobilního internetu stáhla výše uvedená aplikace. Již nainstalovaná aplikace se sama následně otevřela a vygenerovala kód, který jsem následně použil pro přihlášení do internetového bankovnictví klasicky na portálu Fio banky. Po přihlášení na můj účet se nic zvláštního nedělo, vše bylo tak, jak má být.“*

Navrhovatel dále tvrdí, že dne 18. 7. 2014 zjistil neoprávněný převod (přičemž v Protokolu Policie ČR dodává, že se tak stalo v 18:50 hod. při kontrole Účtu v elektronickém bankovnictví) a zablokoval Účet. Navrhovatel tvrdí, že jej zaměstnanec Instituce při telefonním hovoru o blokaci Účtu ubezpečil, že o peněžní prostředky nepřijde, pokud podá trestní oznámení a reklamaci. Navrhovatel popisuje, že dne 18. 7. 2014 podal trestní oznámení a reklamaci.

Navrhovatel zdůrazňuje, že Instituce mu až dne 18. 7. 2014 zaslala upozornění na možnost tohoto napadení, a to pouze do internetového bankovnictví, nikoliv e-mailem nebo jinak.

Navrhovatel v Protestu, který učinil součástí návrhu na zahájení řízení před finančním arbitrem, argumentuje, že k nainstalování viru z podvodného e-mailu došlo i přes řádnou aktualizaci operačního systému použitého počítače a přes ochranu aktualizovaným antivirovým programem. Navrhovatel současně zdůrazňuje, že jako klient Instituce není povinen mít znalosti IT experta, při použití antivirového programu s pravidelnou aktualizací znát jeho přesné vlastnosti, kontrolovat, na jaké viry je právě aktualizován, znát principy šifrování, rozeznávat škodlivé aplikace od bezpečných a bát se otevřít e-mail s přílohou. Navrhovatel má za to, že je to Instituce, kdo je povinen zabezpečit peněžní prostředky svých klientů, přičemž existují metody sledování obvyklého chování klientů, zda se nehlásí z neobvyklé IP adresy nebo nedělají neobvyklou transakci. Instituce by tak mohla takovou transakci zachytit a telefonicky u klienta ověřit, zda ji chce skutečně provést. Navrhovatel dále odkazuje na *„vyjádření odborníků“*: *„Může se jednat o zabezpečení pomocí systémů typu IBM Watson, podvody ze strany klientů může odhalit také obyčejné CRM – třetí reklamace platby v krátkém čase.“*

Navrhovatel v Protestu dále tvrdí, že jej Instituce včas a dostatečným způsobem neinformovala o hrozícím riziku napadení aplikace internetového bankovnictví, konkrétně popisuje, že záložku „Moje zprávy“, kam Instituce Navrhovateli zasílala varování před hrozbami, Instituce obvykle používala k obecným informacím o údržbě systému, nových tarifech, odstávkách, změnách úrokových sazeb atd. Pro informace o vážných bezpečnostních hrozbách považuje Navrhovatel tento způsob informování za nedostatečný, neboť má za to, že kdyby informaci obdržel e-mailem či v podobě vyskakovacího okna v internetovém bankovnictví, k neautorizované platební transakci by v jeho případě nedošlo.

Navrhovatel popisuje, že dne 16. 7. 2014 a před tímto dnem byl jeho počítač Dell Inspiron N5110 Model 5110-9924 (dále jen „Počítač“) s operačním systémem Windows 7 Home

Premium, ID produktu [redacted], chráněn antivirovým programem ESET NOD32 7 Antivirus. Navrhovatel se domnívá, že verze antivirového programu byla ke dni útoku 7.0.317.4, přesnou verzi však z historie záznamů ve svém Počítači již nemůže zjistit. Navrhovatel tvrdí, že se během šetření případu Policií ČR dozvěděl, že na daný typ viru byl tento antivirový program aktualizován až přibližně týden po útoku.

Navrhovatel dále popisuje, že v době útoku používal mobilní telefon zn. Samsung Galaxi Xcover S7710 s operačním systémem Android 4.1 (dále jen „Mobilní telefon Navrhovatele“), který byl chráněn antivirovým programem AVG Antivirus Mobile. Navrhovatel tvrdí, že na Mobilním telefonu Navrhovatele nezměnil nastavení tak, aby na Mobilním telefonu Navrhovatele bylo možno provádět instalaci aplikací z neznámých zdrojů (tedy aplikací, které se nenacházejí na oficiálním úložišti aplikací pro operační systém Android) a současně *„v inkriminovanou dobu neměl na svém mobilním telefonu nainstalovanou žádnou aplikaci, která by nebyla stažena z nabídky „GOOGLE PLAY“*.

Navrhovatel tvrdí, že po provedení sporné platební transakce Počítač předal Policii ČR ke zkoumání a k vytvoření kopie pevného disku. Poté podle doporučení Instituce Počítač odviroval a nadále nepoužíval k přístupu do internetového bankovnictví Instituce. Dále Navrhovatel podle doporučení Instituce uvedl Mobilní telefon Navrhovatele do továrního nastavení a nadále k autorizaci plateb v internetovém bankovnictví používal jiný mobilní telefon.

Navrhovatel se domáhá proti Instituci vrácení peněžních prostředků ve výši 234.520 Kč.

6. Tvrzení Instituce

Instituce potvrzuje, že přijala platební příkaz k převodu částky 234.520 Kč z Účtu na Cílový účet s variabilním symbolem [redacted] a konstantním symbolem [redacted] z IP adresy [redacted] dne 16. 7. 2014 v 11:52:56 hod a v 11:52:57 hod. požadavek o zaslání autorizačního sms kódu.

Instituce tvrdí, že požadovaný sms kód odeslala na telefonní číslo [redacted] v 11:52:59 hod. a v 11:53:37 hod. přijala potvrzení k provedení převodu v podobě autorizačního sms kódu. Instituce potvrzuje, že peněžní prostředky ve výši 234.520 Kč odepsala z Účtu v 11:53:43 hod. a v tentýž okamžik je připsala na Cílový účet.

Instituce namítá, že opakovaně informovala Navrhovatele o hrozících nebezpečích, a tvrdí, že Navrhovatel těmto zprávám nevěnoval pozornost. Instituce dále tvrdí, že na rizika spojená s používáním internetového bankovnictví upozorňuje klienty také v čl. IX., X., XIV. a XV. Podmínek elektronického bankovnictví. Instituce doplňuje, že informace o bezpečnostních hrozbách je možné zjistit také na jejích webových stránkách, konkrétně na přihlašovací stránce internetového bankovnictví pod odkazem „Pravidla bezpečné práce s internetbankingem“.

Instituce namítá, že Navrhovatel si sám aktivně na svá elektronická zařízení nainstaloval škodlivý software, přičemž Instituce své klienty před instalací software z neověřených zdrojů varovala již dne 11. 3. 2014 a 9. 5. 2014.

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 elektronická zařízení a ignorování zpráv zasílaných do internetového bankovnictví i standardních obezřetnostních zásad průměrného uživatele informačních technologií, jako hrubou nedbalost, která způsobila

vyzrazení dvou personalizovaných bezpečnostních prvků platebního prostředku, tedy hesla pro přístup do internetového bankovnictví a autentizačního kódu sloužícího k autorizaci provedené platební transakce.

Instituce doplňuje, že způsob provedení phishingových útoků je již po několik let silně medializován a zásada neotevírat přílohy z neznámých zdrojů a neinstalovat do elektronických zařízení programy z neověřených zdrojů je notoricky známá.

Instituce argumentuje, že ztrátu z platební transakce, která je předmětem sporu, nese v tomto případě Navrhovatel podle § 116 odst. 1 písm. b) zákona o platebním styku a nikoli Instituce.

Instituce současně odkazuje na zjištění Policie ČR o tom, jakým způsobem dochází k napadení počítačů, z nichž pak útočník získá informace k internetovému bankovnictví a další údaje, které zneužije k odčerpání peněžních prostředků bez vědomí osoby oprávněné s účtem disponovat. Instituce popisuje, že podle zjištění Policie ČR nejsou v případě Navrhovatele k dispozici žádné specifické informace o průběhu útoku, avšak Policie ČR konstatuje, že jde o stejný způsob napadení elektronických zařízení, jako v ostatních případech realizovaných ve stejné vlně phishingových útoků realizovaných stejným malware. Instituce tak má za to, že Navrhovatel musel aktivně nainstalovat malware do svých elektronických zařízení, tedy rozkliknout a instalovat přílohu podvodného e-mailu a následně aktivně instalovat malware z neověřeného zdroje, vydávající se za aplikaci pro internetové bankovnictví, do svého mobilního telefonu, a to přes varovná hlášení, resp. musí nadto změnit tovární nastavení telefonu tak, aby tato instalace byla vůbec možná.

Instituce připouští, že majitel Cílového účtu jí výběry peněžních prostředků převedených při Sporné platební transakci předem neohlásil, a vysvětluje, že povinnost hlásit výběry hotovosti předem má za cíl zajištění dostatečné likvidity jejích poboček. Pokud však zaměstnanci pobočky mají za to, že konkrétní výběr nebude mít vliv na plynulost provozu pobočky, nemá Instituce povinnost výběr odmítnout. Instituce popisuje, že majitel Cílového účtu výběry provedl ve výši 100.000 Kč na pobočce Instituce na adrese V Celnici 1028/10, 117 21 Praha 1, 100.000 Kč na pobočce Instituce na adrese Moskevská 268/53, 101 00 Praha 10 a 34.000 Kč na pobočce Instituce na adrese Ječná 35, 120 00 Praha 2. Těmto pobočkám Instituce nestanovila specifická pravidla pro výběry hotovosti.

7. 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 podklady pro své rozhodnutí; při svém rozhodování vychází ze skutkového stavu věci a volně hodnotí shromážděné podklady.

Navrhovatel se domáhá, aby mu Instituce vrátila peněžní prostředky ve výši 234.520 Kč, které zaúčtovala k tíži jeho Účtu na základě platebního příkazu, který nezadal.

7.1 Skutková zjištění

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

a) Dne 15. 7. 2014 v 23:30 hod. Navrhovatel přijal a následně otevřel připojenou přílohu zprávy elektronické pošty, přesněji e-mail s přílohou ve formátu ZIP s názvem

„prikaz3D866ED727D82620F.zip“; text tohoto e-mailu zněl: *„Soudní exekutor Grosam, Jan, JUDr., Exekutorský úřad Sokolov město, IČ 703277789, sídlo U Divadla 216, 306 01 Sokolov pověřený provedením exekuce: č.j.* [redacted]*, a ustanovení: Příkaz č.j.* [redacted] *V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění výše uvedených povinností, které ukládá ustanovení, jakož 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: 9 548,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 045,00 Kč včetně DPH 21% Náklady exekuce paušálem: 3 201,00 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 13 794,00 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“);

b) Dne 15. 7. 2014 v 23:35:13 hod. došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted] a ke kontrole zůstatku na Účtu, v 23:39:03 hod. uživatel opět zkontroloval zůstatek na Účtu a v 23:42:30 hod. a v 23:42:34 hod. zkontroloval pohyby na Účtu. V 23:42:39 hod. se uživatel z internetového bankovnictví Navrhovatele odhlásil.

c) Dne 16. 7. 2014 v 4:55:40 hod. došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted] a v 4:55:40 hod. a v 4:56:13 hod. ke kontrole zůstatku na Účtu.

d) Dne 16. 7. 2014 v 8:29:37 hod. došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted]; při tomto přihlášení došlo v 8:29:38 hod. ke kontrole zůstatku na Účtu, v 8:29:44 hod., v 8:30:01 hod. a v 8:31:55 hod. ke kontrole pohybů na Účtu, v 8:32:12 hod. k zobrazení smluv, v 8:32:21 hod. k zobrazení globálního nastavení a v 8:32:42 hod. a v 8:36:51 hod. k zobrazení informací o Účtu.

e) Dne 16. 7. 2014 v 11:44:48 hod. došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted] a v 11:44:49 hod. ke kontrole zůstatku na Účtu, které Navrhovatel tvrdí, že neprovedl (dále jen „Sporné přihlášení“). Při Sporném přihlášení došlo celkem 14krát ke kontrole zůstatku Účtu a jednou k zobrazení globálního nastavení. V 11:52:56 hod. byl zadán platební příkaz k převodu částky 234.520 Kč na Cílový účet a v 11:53:37 hod. byl potvrzen zadáním autorizačního sms kódu (dále jen „Sporná platební transakce“).

f) Instituce dne 16. 7. 2014 v 11:53:43 hod. provedla Spornou platební transakci, tedy odepsala peněžní prostředky ve výši 234.520 Kč z Účtu a v tentýž okamžik je připsala na Cílový účet.

g) Dne 16. 7. 2014 došlo po Sporném přihlášení k přihlášení do internetového bankovnictví Navrhovatele ještě celkem 9x, z toho
   (i) 6x z IP adresy [redacted] (tedy z IP adresy použité při Sporném přihlášení a při zadání Sporné platební transakce) v čase 12:41:10 hod. až 14:58:41 hod.; při těchto přihlášeních uživatel vždy zkontroloval zůstatek na Účtu, pohyby na Účtu nebo informace o Účtu;
   (ii) jednou z IP adresy [redacted] v čase 14:59:12 hod.; při tomto přihlášení uživatel zkontroloval zůstatek na Účtu, pohyby na Účtu a výpisy z Účtu;
   (iii) jednou z IP adresy [redacted] (tedy z IP adresy použité při Sporném přihlášení a při zadání Sporné platební transakce) v čase 15:04:13 hod.; při tomto přihlášení uživatel

zkontroloval pohyby na účtu a v 15:11:28 hod. zadal platební příkaz k převodu částky 292.344 Kč z jiného účtu Navrhovatele č. [redacted] na účet č. [redacted]; Instituce k tomuto platebnímu příkazu zaslala v 15:11:29 hod. a v 15:14:35 hod. autorizační sms zprávu, avšak uživatel tento příkaz zadáním autorizačního sms kódu nepotvrdil;

(iv) jednou z IP adresy [redacted] v čase 21:43:55 hod.; při tomto přihlášení uživatel zkontroloval zůstatek na Účtu, pohyby na Účtu, přehled příkazů a výpisy z Účtu.

h) Instituce Spornou platební transakci zúčtovala k tíži Účtu dne 16. 7. 2014 s datem účtování i datem transakce *„16.7.2014“*, ID operace *„[redacted]“*, operace *„Platba převodem“*, zpráva pro příjemce *„zaloha“*, číslo protiúčtu číslo Cílového účtu, variabilní symbol *„[redacted]“*, konstantní symbol *„[redacted]“* a částka *„-234 520,00“*.

i) Dne 17. 7. 2014 nedošlo k žádnému přihlášení do internetového bankovnictví Navrhovatele.

j) Dne 18. 7. 2014 v 9:59:38 hod. došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted]; při tomto přihlášení došlo ke kontrole zůstatku na Účtu, ke kontrole pohybů na Účtu a ke kontrole výpisů z Účtu. Dále v tento den došlo k přihlášení do internetového bankovnictví Navrhovatele v 18:37:21 hod. opět z IP adresy [redacted]; při tomto přihlášení došlo ke kontrole zůstatku na Účtu, ke kontrole pohybů na Účtu a ke kontrole přehledu příkazů.

k) Dne 18. 7. 2014 v 18:51:51 hod. došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted]; při tomto přihlášení došlo k zobrazení přehledu příkazů. Finanční arbitr má za to, že toto přihlášení provedl Navrhovatel, neboť Navrhovatel tvrdí, že provedení Sporné platební transakce zjistil dne 18. 7. 2014 v 18:50 hod., a finanční arbitr zjistil, že toto přihlášení má úzkou časovou souvislost s telefonickým hovorem Navrhovatele s Institucí dne 18. 7. 2014 v 18:59:22 hod., o kterém Instituce tvrdí, že jí v něm Navrhovatel oznámil Spornou platební transakci.

Finanční arbitr nemá telefonický hovor ze dne 18. 7. 2014 v 18:59:22 hod. k dispozici, neboť Instituce tvrdí, že jeho záznam je poškozen, a současně předložila poškozenou nahrávku, kterou nelze přehrát. Finanční arbitr však na jeho obsah usuzuje z telefonického hovoru z téhož dne v 19:01:54 hod., který na telefonický hovor ze dne 18. 7. 2014 v 18:59:22 hod. bezprostředně navázal.

Skutečnosti uvedené v bodu a) vyplývají ze screenshotu e-mailu od exekutora, který finančnímu arbitrovi předložil Navrhovatel, a jeho tvrzení. Skutečnosti uvedené v bodu h) vyplývají z výpisu z Účtu za měsíc červenec 2014, který předložil finančnímu arbitrovi Navrhovatel.

Skutečnosti popsané v bodech b) až g) a i) až j) vyplývají z podkladů, které předložila Instituce [konkrétně z Přehledu přístupů do IB, Přehledu aktivit v IB, Přehledu aktivit v IB od 17. 7. 2014 do 18. 7. 2014, 3 otisků informačního systému Instituce se zobrazením informací o platební transakci ve výši 234.520 Kč ze dne 16. 7. 2014 (tedy o Sporné platební transakci), 3 otisků informačního systému Instituce se zobrazením informace o neprovedené platební transakci ve výši 292.344 Kč ze dne 16. 7. 2014].

Skutečnosti popsané v bodě k) vyplývají kromě výše citovaných podkladů Instituce také z tvrzení Navrhovatele a 3 otisků informačního systému Instituce se zobrazením informace o datu a čase začátku a konce telefonických hovorů mezi Navrhovatelem a Institucí.

7.2 Autorizace platební transakce

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.“*

Souhlas s platební transakcí může 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, nemusí se jednat 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).*

7.3 Sporná platební transakce jako neautorizovaná platební transakce

Navrhovatel tvrdí, že Spornou platební transakci nezadal, tedy že ji neautorizoval.

Instituce předložila Přehled aktivit v IB, který v tomto případě dokládá, že Sporná platební transakce byla provedena po úspěšném přihlášení do internetového bankovnictví Navrhovatele (to vyplývá ze záznamu *„16.07.2014 11:44:48 Přihlášení do aplikace“*) a za použití autorizačního sms kódu (to vyplývá ze záznamu *„16.07.2014 11:53:37 Úspěšná autorizace*

pokynu SMS“). Instituce tímto prokázala, že při Sporné platební transakci byla dodržena dohodnutá forma a postup.

Protože ale skutkové okolnosti případu, zejména zjištění Policie ČR týkající se Počítače, nasvědčují tomu, že Navrhovatel příkaz k provedení Sporné platební transakci nemusel zadat, bude se finanční arbitr Spornou platební transakcí zabývat jako platební transakcí neautorizovanou, se kterou zákon o platebním styku spojuje právní následky v podobě speciální odpovědnosti poskytovatele nebo uživatele platebních služeb za neautorizovanou platební transakci.

7.4 Odpovědnost 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, ve smyslu § 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 o 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.“*

7.5 Odpovědnost za Spornou platební transakci jako neautorizovanou platební transakci

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 11:52:56 hod. a v 11:53:37 hod. potvrzen zadáním autorizačního sms kódu;
(ii) Instituce Spornou platební transakci provedla dne 16. 7. 2014 v 11:53:43 hod.;
(iii) Navrhovatel dne 18. 7. 2014 v 18:59:22 hod. kontaktoval telefonicky Instituci;

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

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 224 346 797. Přestože ze 3 otisků informačního systému Instituce se zobrazením informace o datu a čase začátku a konce telefonických hovorů mezi Navrhovatelem a Institucí vyplývá, že Navrhovatel k oznámení zneužití internetového bankovnictví využil linku 224 346 777, z vyjádření obou stran sporu ani z podkladů shromážděných finančním arbitrem nevyplynulo, že by linka s telefonním číslem 224 346 797 nebyla v rozhodné době pro tento případ v provozu nebo že by se Navrhovatel pokoušel kontaktovat Instituci na lince 224 346 797 a nepodařilo se mu to.

Použití ustanovení § 116 odst. 2 zákona o platebním styku tedy v projednávaném případě nepřichází v úvahu.

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"*.

Navrhovatel si zvolil uživatelské jméno a heslo pro první přihlášení ve Smlouvě o elektronickém bankovnictví. Smlouva o elektronickém bankovnictví současně ve svém čl. II. odst. 3. stanoví, že Navrhovatel 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 Navrhovateli. 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 povinnosti podle § 102 odst. 1 písm. a) zákona o platebním styku Instituce nezajistila.

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“.*

Navrhovatel tvrdí, že počítačový vir napadl jeho elektronická zařízení a finančnímu arbitrovi k tomu předložil screenshot E-mailu od exekutora, Vyjádření Policie ČR a Usnesení. Z těchto podkladů vyplývá, že Policie ČR poté, co jí Navrhovatel odevzdal Počítač ke zkoumání, vytvořila bitovou kopii jeho disku, kterou prohlédla a konstatovala, že v Počítači byl nainstalován škodlivý software, tzv. malware, a že konkrétně se jednalo o *„downloader obsažený v souboru, který byl přílohou e-mailové zprávy týkající se neexistující exekuce, a tento se spustil v okamžiku, kdy se uživatel pokoušel přílohu otevřít. Downloader pak stáhl, a spustil další malware, jejichž účelem je získat informace o internetovém bankovnictví, užívaných účtem a přihlašovacích údajích a upravující běžné stránky bankovních institucí, do nichž pak je vložen odkaz na instalaci aplikace do „chytrého“ mobilního telefonu, jejímž účelem je odchycení potvrzovacích kódů pro platby.“*

Policie ČR ve Vyjádření Policie ČR dále popisuje, jak k podobným útokům dochází:

„- Občan obdrží podvodný e-mail, jehož přílohou je soubor ve formátu ZIP
- *Soubor formátu ZIP obsahuje rtf dokument se krytým exe souborem (tzv. downloader), ten stahuje na pozadí z internetu do napadeného počítače další škodlivé soubory (malware), zodpovědné za krádeže hesel a peněz, tyto kompletní backdoory, dovolují kradení dat, vzdálené připojení, spouštění a stahování dalších souborů, počítač je pak pod plnou „nadvládou“ útočníka, mimo jiné se může jednat i o úpravu stránky internetového bankovnictví – přidání hlášky o doporučení instalace aplikace do telefonu – ta je pak odpovědná za odchytávání potvrzovacích kódů pro platby*
- *Tento malware vyčkává cca 7 minut, uživatel si čte smlouvu*
- *Po cca 7 minutách se infikovaný počítač spojí s cca 5 URL adresami, ze kterých stahuje hlavní funkcionalitu, jedná se o domény se Francii, Polsku, Brazílii a další*
- *Zde se jedná se o stránky většinou na jedno použití, přístupové údaje jsou smyšlené, většinou za stránky není ani zaplaceno*
- *Zmíněných cca 5 URL (s viry typu trojského koně Zbot, Tinba, Papras ...) komunikuje s jednou IP adresou*
- *V PC se vyskytne tzv. Passportstealer, hledá hesla, e-maily, adresy, je možné také spuštění VNC klienta (ovládání PC na dálku)*
- *Nyní je PC plně pod kontrolou útočníka*
- *Nainstalovaný malware si hlídá některé web stránky, např. FIO banky a další seznam adres, které jsou pro útočníka zajímavé*
- *Útočník podvrhne jím vytvořenou webovou stránku (okno, html kod – upravený print screen daného elektronického bankovnictví)*
- *Uživateli je vnucena instalace mobilní aplikace, objeví se např. okno pro zvýšení zabezpečení a kvality si nainstalujte… útočník potřebuje spárovat telefon s PC*

- *Uživatel si stáhne aplikaci, např. TrusteerServis24.apk (je možné, že uživatel obdrží také sms zprávu s adresou, ze které si má stáhnout závadný instalační software)*
- *Po uživatelově nainstalování závadné aplikace do mobilu, dochází k vygenerováním kódu*
- *Vygenerovaný kód z nainstalované mobilní aplikace uživatel zadá na podvodné stránky ve svém PC, tím dojde ke spárování jeho PC a TLF k danému bankovnímu účtu*
- *Je aktivován tzv. Backdoor, mobilní telefon přeposílá sms zprávy, na účet uživatele, na jiné tel číslo*
- *Potvrzovací sms zpráva pro finanční převody a transakce je již pod nadvládou útočníka*
- *Bez vygenerovaného potvrzovacího kódu nedojde ke spárování telefonu a PC, až po spárování má útočník plnou kontrolu nad internetovým bankovnictvím.“*

Výše popsaný průběh útoku odpovídá tvrzením Navrhovatele obsaženým v Protokolu Policie ČR.

Všechny dosud shromážděné podklady nasvědčují závěru, že si Navrhovatel otevřením přílohy E-mailu od exekutora nainstaloval do Počítače výše popsaný malware, který jej při dalším přihlášení do internetového bankovnictví (a to s největší pravděpodobností dne 15. 7. 2014 v 23:35:13 hod.) vyzval k instalaci dalšího malware do Mobilního telefonu Navrhovatele, a tím útočník získal přístup k přihlašovacím údajům do internetového bankovnictví a autorizačním sms zasílaným Institucí na Mobilní telefon Navrhovatele.

Všechny dosud shromážděné podklady tedy svědčí závěru, že ke zneužití internetového bankovnictví Navrhovatele došlo ve sféře Navrhovatele, a to napadením elektronických zařízení, na kterých Navrhovatel používal internetové bankovnictví. Ze shromážděných podkladů současně 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.

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:* [redacted] *(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: [redacted]], 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 v běžném e-mailovém styku mnoho e-mailů, které žádné bezpečnostní riziko nepředstavují (např. předem nesmluvený e-mail od známé osoby, jejíž e-mailovou adresu adresát dosud nezná). 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:

a) 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;

b) 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), antivirovým programem a pravidelně jej aktualizovat, popř. povinnost chránit počítač legálním firewallem;
c) 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;
d) 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;
e) 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;
f) 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 by tedy za ztrátu ze Sporné platební transakce odpovídal, pokud by ji způsobil svým podvodným jednáním, nebo pokud by některou z povinností uvedených v bodech a) až f) 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.

Finanční arbitr nezjistil, že by Navrhovatel ztrátu ze Sporné platební transakce způsobil svým podvodným jednáním.

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. 3. 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.

Ad a)

Finanční arbitr nezjistil, že by Navrhovatel porušil povinnost uvedenou shora pod bodem a). Navrhovatel v Protokolu Policie ČR tvrdí, že když se do internetového bankovnictví hlásil *„jako obvykle"*, tak jej k instalaci aplikace do mobilního telefonu vyzvalo vyskakovací okno. Z toho nelze usuzovat, že by se Navrhovatel v tu chvíli nenacházel na internetových stránkách Instituce. Navrhovatel sice tvrdí, že mu aplikace nainstalovaná v Mobilním telefonu Navrhovatele vygenerovala kód, který následně použil pro přihlášení do internetového bankovnictví *„klasicky na portálu Fio banky"*. Finanční arbitr má pochybnosti, že by Navrhovatel tento kód skutečně zadával na portálu Instituce, avšak i kdyby ho Navrhovatel zadával na jiné webové stránce, tak z tohoto tvrzení nevyplývá, že by takto zadával personalizované bezpečnostní prvky.

Ad b) a c)

Navrhovatel tvrdí, ale nedokládá, že měl Počítač před provedením Sporné platební transakce chráněn antivirovým programem ESET NOD32 7 Antivirus, pravděpodobně verze 7.0.317.4, a Mobilní telefon Navrhovatele měl chráněn antivirovým programem AVG Antivirus Mobile.

Ze shromážděných podkladů však současně nevyplývá, ani to Instituce netvrdí, že by Navrhovatel způsobil ztrátu ze Sporné platební transakce tím, že by neměl svá elektronická zařízení chráněna aktualizovaným antivirovým programem. Nadto 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.

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 d)

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 před provedením Sporné platební transakce nevěnoval pozornost žádnému z bezpečnostních upozornění, které mu do internetového bankovnictví zaslala Instituce, neboť si žádné z těchto bezpečnostních upozornění ani neotevřel (resp. otevřel si je až po provedení Sporné platební transakce). To vyplývá z bezpečnostních upozornění, která Instituce zaslala do internetového bankovnictví Navrhovatele od 8. 10. 2013 do 25. 2. 2015 a 2 otisků informačního systému Instituce se zobrazením informace o přečtení bezpečnostních upozornění.

Finanční arbitr nesouhlasí s Navrhovatelem, pokud tvrdí, že mu Instituce tato bezpečnostní upozornění měla zasílat e-mailem. Navrhovatel se s 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 8 bezpečnostních upozornění, a to ve dnech 8. 10. 2013, 19. 12. 2013, 28. 1. 2014, 7. 3. 2014, 11. 3. 2014, 9. 5. 2014, 5. 6. 2014 a 23. 6. 2014. Bezpečnostní upozornění z 8. 10. 2013 mu v internetovém bankovnictví zobrazovala do 30. 12. 2013 (tedy po dobu více než 2 měsíců), 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 9. 4. 2015, kdy je finančnímu arbitrovi předložila.

Dne 8. 10. 2013 Instituce zaslala Navrhovateli varování tohoto znění: *„Vážení klienti,

 jelikož se v nedávné době napříč celým tuzemským bankovním sektorem vyskytla řada více či méně úspěšných pokusů o cílené zneužití platebních nástrojů klientů bank, dovolujeme si Vám touto cestou poukázat na některé bezpečnostní zásady, jejichž dodržování je tou nejlepší prevencí před vznikem škody.
 Případy, o které se jedná, jsou souhrnně nazývány "phishing" a jejich společným znakem je snaha pachatele získat od klienta banky jeho autorizační údaje k platební kartě, elektronickému bankovnictví či jinému elektronickému platebnímu prostředku. Nekalé praktiky na bázi phishingu se v zásadě dají rozdělit na dvě skupiny:
 1) Pokus vylákat autorizační údaje vytvořením dojmu, že klient komunikuje se svojí bankou
 2) Pokus získat autorizační údaje prostřednictvím elektronických nástrojů, např. virů

 Obrana před oběma formami phishingu je velmi prostá, vyžaduje však ze strany klienta, tj. držitele platebního nástroje, důsledné dodržování bezpečnostních zásad, z nichž ty nejdůležitější Vám nyní tímto chceme v zájmu ochrany Vašich peněžních prostředků připomenout:
 - Nikdy nesdělujte jakékoliv autorizační údaje (login a heslo k internetbankingu, číslo platební karty, datum platnosti karty, CVC/CVV kód z rubu karty, PIN ke kartě apod.) třetím osobám. Pokud se jakákoliv osoba vydává za zástupce banky a požaduje po Vás sdělení některého z těchto údajů,*

*jedná se s největší pravděpodobností o pokus o podvod ! Fio banka po Vás nikdy nebude chtít takové údaje sdělit, nanejvýše může jako součást identifikace na dálku chtít sdělit určitou sekvenci z čísla platební karty, nikdy však celé její číslo.
 - V prostředí internetu zadávejte autorizační údaje k platební kartě pouze na důvěryhodných platebních branách. Nikdy nevyplňujte formuláře vyžadující sdělení autorizačních údajů ke kartě, jež nemají přímou souvislost s prováděním platebních transakcí. Fio banka Vám nikdy nebude předkládat k vyplnění formulář sdělující, že údaje potřebuje z důvodu jejich ověření, což je poměrně obvyklá mystifikace ze strany pachatelů elektronického phishingu.
 - Důsledně chraňte svoje prostředky elektronické komunikace (PC, notebook, tablet, mobilní telefon atd.) vhodným antivirovým programem před elektronickými útoky z venčí. Z nechráněného zařízení může vzdálený útočník snadno získat jakékoliv Vaše autozizační údaje, které na něm zadáváte.
 - Neotvírejte přílohy e-mailů a neinstalujte aplikace z nedůvěryhodných zdrojů. Zejména pro chytré telefony platí, že každý jejich uživatel by si měl aplikace stahovat výhradně z příslušných oficiálních aplikačních marketů.
 Závěrem připojujeme <A HREF="https://www.czech-ba.cz/sites/default/files/dokumentyclanku/ceska-bankovni-asociace-varuje-pred-novou-formou-hackerskych-utoku/04102013tzcbaceskabankovniasociacevarujeprednovouformouhackerskych utokufinal.pdf" >odkaz na Tiskovou zprávu</A> České bankovní asociace z 4.10.2013, která vzrůstající riziko phishingu vnímá rovněž velmi vážně a považuje za nezbytné dát tomuto tématu dostatečnou publicitu.

 Váš tým klientské podpory.
“*

Dne 19. 12. 2013 Instituce zaslala Navrhovateli varování tohoto znění: *„Vážení klienti, vzhledem k přetrvávajícímu vysokému stupni rizika tzv. phishingových útoků na bankovní účty, na nějž jsme Vás touto cestou upozorňovali již zprávou ze dne 8.10.2013 (jejíž úplné znění je pro všechny nyní k dispozici ZDE), bychom Vám rádi připomněli zásady prevence, abyste se právě Vy obětí takového útoku nestali. Veškerá elektronická zařízení, na nichž provozujete aplikace Internetbanking a Smartbanking, mějte trvale chráněna účinným a pravidelně aktualizovaným antivirovým programem. Virus, 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 Vašeho telefonu, aby pro pachatele získal autorizační SMS k potvrzení převodního příkazu zadaného na napadeném účtu. 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 znám 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 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 Vašeho internetového bankovnictví. 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.“*

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: +420 224 346 777 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, obsahují varování ze dne 8. 10. 2013, 19. 12. 2013 a 28. 1. 2014 jasné a srozumitelné informace a pokyny, jimiž se Navrhovatel v tomto případě stejně neřídil. Jedná se konkrétně o pokyn, aby uživatel neotevíral přílohy e-mailů, jež pocházejí od neznámých adresátů, 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, viz níže). 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 byly odeslány dne 8. 10. 2013, 19. 12. 2013 a 28. 1. 2014, neztratily nic na své aktuálnosti ani ke dni provedení Sporné platební transakce.

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 8. 10. 2013, 19. 12. 2013 a 28. 1. 2014 obsahovala dostatek informací a pokynů, při jejichž dodržení by Navrhovatel provedení Sporné platební transakce s největší pravděpodobností zabránil.

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

Ad e)

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 tak povinnost stanovenou v čl. XIV., odst. 5 Podmínek elektronického bankovnictví neporušil.

Finanční arbitr však nemůže přisvědčit námitce Navrhovatele, že jako klient Instituce není povinen bát se otevřít e-mail s přílohou. Povinností Navrhovatele podle Smlouvy o elektronickém bankovnictví naopak je vždy posoudit, zda došlý e-mail nemá podezřelý název nebo obsah, a to zejména jde-li o e-mail od neznámého adresáta. U takového e-mailu je Navrhovatel zejména povinen vyvarovat se otevření přílohy.

Ad f)

Navrhovatel tvrdí, že výzvu k instalaci „bezpečnostní aplikace“ na Mobilní telefon Navrhovatele obdržel prostřednictvím sms, u které byl jako odesílatel uveden „INFO“ a text zprávy zněl: *„Odkaz: [redacted]“*. Finanční arbitr proto vylučuje, že by mohlo jít o aplikaci pocházející z oficiálního úložiště pro Android – Google Play (resp. Obchod Play). Jestliže tedy Navrhovatel aplikaci do Mobilního telefonu Navrhovatele stáhl z tohoto odkazu, pak se mýlí, tvrdí-li, že „*v inkriminovanou dobu neměl na svém mobilním telefonu nainstalovanou žádnou aplikaci, která by nebyla stažena z nabídky „GOOGLE PLAY“*.

Finanční arbitr měl původně v úmyslu provést ohledání Mobilního telefonu Navrhovatele, avšak Navrhovatel finančnímu arbitrovi sdělil, že ho k doporučení Instituce uvedl do továrního nastavení. Finanční arbitr proto provedl zkoumání mobilního telefonu značky Samsung Galaxy Xcover S7710 2, sériové číslo [redacted], s operačním systémem Android, verze 4.1, a nainstalovaným antivirovým programem AVG (dále jen „Testovací telefon“), jako nejbližšího dostupného modelu k Mobilnímu telefonu Navrhovatele. Finanční arbitr akceptoval ohledání Testovacího telefonu, neboť účelem zkoumání bylo zjistit postup instalace aplikace z neověřeného zdroje, tedy skutečnost, která závisí na operačním systému telefonu a jeho konkrétní verzi, která byla u Testovacího telefonu stejná jako u Mobilního telefonu Navrhovatele.

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. Navrhovatel tvrdí, že na Mobilním telefonu Navrhovatele nezměnil nastavení tak, aby na Mobilním telefonu Navrhovatele bylo možno provádět instalaci aplikací z neznámých zdrojů (tedy aplikací, které se nenacházejí na úložišti Google Play, resp. Obchod Play).

Pokud uživatel na Testovacím telefonu stáhne jakoukoliv aplikaci, která nepochází z Google Play, pak při pokusu o její instalaci Testovací telefon zobrazí upozornění: *„Instalace byla zablokována. Z důvodu zabezpečení je telefon nastaven tak, že blokuje instalaci aplikací, které nepocházejí z Google Play“* Tento text je doprovázen tlačítky *„Zrušit“* (jako první v řadě) a *„Nastavení“*. Klikne-li uživatel na tlačítko *„Nastavení“*, bude mít možnost v sekci Zabezpečení zakliknout položku Neznámé zdroje. Pokud tak učiní, Telefon zobrazí upozornění: *„Neznámé zdroje. Vaše zařízení a osobní údaje jsou zranitelnější vůči útokům aplikací z neznámých zdrojů. Souhlasíte s tím, že nesete plnou odpovědnost za jakékoli poškození zařízení nebo ztrátu dat způsobené použitím těchto aplikací.“* Tento text je doprovázen tlačítky *„Zrušit“* (jako první v řadě) a *„OK“*. Klikne-li uživatel na tlačítko *„OK“*, bude již moci aplikaci z neznámého zdroje nainstalovat. Testovací telefon při instalaci zobrazí text: *„Chcete nainstalovat tuto aplikaci? Povolit tuto aplikaci:“* 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.

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 (Navrhovatel pouze tvrdí, že si Počítač a Mobilní telefon Navrhovatele chránil antivirovým programem, tyto skutečnosti však nijak nedoložil) 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 elektronickém bankovnictví zaslala (přestože mu je Instituce v internetovém bankovnictví zobrazovala po dobu několika měsíců, popř. dosud). Finanční arbitr považuje takovou nečinnost Navrhovatele za hrubou nedbalost, neboť projevil naprostý nezájem o bezpečnostní otázky.

V případě instalace aplikace dospěl finanční arbitr k závěru, že Navrhovatel jednal hrubě nedbale, neboť Navrhovatel si musel vzhledem k výše citovaným upozorněním zobrazeným na Mobilním telefonu Navrhovatele 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. Tím spíš by tak učinil

za situace, kdy by se nemohl do internetového bankovnictví přihlásit dohodnutým způsobem. 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. Pokud tedy Navrhovatel tvrdí, že *„[j]iž nainstalovaná aplikace se sama následně otevřela a vygenerovala kód, který jsem následně použil pro přihlášení do internetového bankovnictví“,* měl Navrhovatel považovat za podezřelé, že se nemůže přihlásit do svého internetového bankovnictví sjednaným způsobem, a kód nezadávat, dokud si neověří bezpečnost takového kroku.

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.

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 to 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, a 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.

7.6 Ostatní námitky Navrhovatele

Finanční arbitr Navrhovateli přisvědčuje, že ho Instituce nesprávně informovala o tom, že o peněžní prostředky ze Sporné platební transakce nepřijde. To totiž vyplývá ze záznamu telefonního hovoru s názvem *„3287929.wav“*, kde zaměstnanec Instituce tvrdí: *„banka potom bude vědět, odkud kam ty peníze a poskytne vám součinnost, ano, abyste ty peníze dostal zpátky, abyste byl v tomto směru klidný.“* Na Navrhovatelův dotaz, od koho peníze dostane zpátky, zaměstnanec Instituce odpověděl: *„Od banky“*. Na další Navrhovatelův dotaz, zda o tyto peněžní prostředky nepřijde, zaměstnanec Instituce odpověděl: *„Ne, nepřijdete o ty peníze, ano, to jsem vás chtěl uklidnit“*.

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.

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.

Instituce nebyla povinna Spornou platební transakci jako neobvyklou neprovést a nejprve ověřit u Navrhovatele. Podle § 105 odst. 1 zákona o platebním styku platí, že *„[p]oskytovatel může odmítnout provést platební příkaz pouze tehdy, nejsou-li splněny podmínky pro jeho provedení, nebo stanoví-li tak jiný právní předpis. Poskytovatel je povinen odmítnout provedení platebního příkazu, stanoví-li tak jiný právní předpis…“* Navrhovatel si s Institucí v čl. XII. „Nakládání s peněžními prostředky na účtu“, odst. 13 Podmínek vedení účtů dohodl: *„[b]anka* (tedy Instituce – pozn. finančního arbitra) *může odmítnout provést dispozici s peněžními prostředky na účtu, pokud je v rozporu se Smlouvou, těmito podmínkami, závaznými právními předpisy nebo s rozhodnutím soudních či správních orgánů.“* Skutečnost, že uživatel zadá neobvyklý platební příkaz, by mohla v Instituci vzbudit podezření, že nejsou splněny podmínky pro provedení platebního příkazu ve smyslu § 105 odst. 1 zákona o platebním styku a čl. XII. odst. 13 Podmínek vedení účtů, konkrétně že souhlas s platební transakcí neudělil Navrhovatel. Zákon o platebním styku a Smlouva o účtu však dávají Instituci právo, nikoliv povinnost neprovést platební příkaz při podezření na neautorizovanou platební transakci. Žádný jiný právní předpis pak nestanoví, že je Instituce povinna odmítnout provést platební příkaz k neobvyklé platební transakci. Zákon o platebním styku a Smlouva o účtu tak Instituci neukládají odkládat přijetí platebního příkazu na dobu, než si ověří, zda jej zadal Navrhovatel.

Své tvrzení, že Instituce měla internetové bankovnictví zabezpečit *„pomocí systémů typu IBM Watson“*, Navrhovatel nijak blíže nevysvětlil a Instituce se k němu nijak nevyjádřila, tato námitka je tak zcela neurčitá. Finanční arbitr může pouze konstatovat, že takové zabezpečení Instituci žádný právní předpis neukládá. Totéž platí o použití *„obyčejného CRM“*, kdy z Navrhovatelova tvrzení nadto vyplývá, že tento systém má sloužit nikoliv k odhalení podvodů ze strany třetích osob, ale podvodů ze strany samotných klientů.

Konečně, k námitce Navrhovatele, že Instituce neměla umožnit majiteli Cílového účtu vybrat z Cílového účtu hotovost převyšující 50.000 Kč, finanční arbitr zjistil, že majitel Cílového účtu a Instituce si v čl. XI. odst. 11. Obchodních podmínek k Rámcové smlouvě o poskytování platebních služeb účinných ode dne 20. 6. 2014, které jsou nedílnou součástí Rámcové smlouvy o poskytování platebních služeb, kterou mezi sebou uzavřeli dne 10. 7. 2014, dohodli, že majitel účtu je povinen výběry z Cílového účtu v celkovém součtu nad 100.000 Kč nepřevyšující částku 500.000 Kč hlásit Instituci nejpozději dva pracovní dny před jejich splatností. Toto ustanovení však nestanoví Instituci povinnost neohlášené výběry neprovést. Rámcová smlouva o poskytování platebních služeb ze dne 10. 7. 2014 pak žádné limity výběrů hotovosti neupravuje. Instituce tak provedením výběrů neporušila žádnou právní povinnost.

8. <u>K výroku rozhodnutí</u>

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

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 15. 1. 2016

otisk úředního razítka

Mgr. Monika Nedelková
finanční arbitr