F i n a n č n í a r b i t r

Legerova 1581/69, 110 00 Praha 1 – Nové Město, Tel. +420 257 042 094,
ID datové schránky: qr9ab9x, e-mail: arbitr@finarbitr.cz, https://www.finarbitr.cz

Navrhovatel
[redacted]

Instituce
Česká spořitelna, a.s.
IČO 452 44 782
Olbrachtova 1929/62
140 00 Praha 4

Č. j. FA/SR/PS/1490/2016 - 14
Praha 26. 10. 2018

N á l e z

Finanční arbitr příslušný k rozhodování sporů podle § 1 odst. 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. 7. 2016 podle § 8 odst. 1 zákona o finančním arbitrovi na návrh Navrhovatele proti Instituci, vedeném podle tohoto zákona a zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, o zaplacení částky 152.000 Kč, takto:

I. Řízení o návrhu navrhovatele, [redacted], se v části o zaplacení částky 12.000 Kč (slovy: dvanáct tisíc korun českých) podle § 14 odst. 1 písm. c) zákona o finančním arbitrovi zastavuje.

II. Návrh navrhovatele, [redacted], se v části o zaplacení částky 140.000 Kč (slovy: jedno sto čtyřicet tisíc korun českých), podle § 15 odst. 1 zákona o finančním arbitrovi zamítá.

Odůvodnění:

1 Předmět řízení před finančním arbitrem a zkoumání podmínek řízení

Navrhovatel se po Instituci domáhá vrácení částek platebních transakcí, které Instituce provedla na základě platebních příkazů zadaných prostřednictvím jeho internetového bankovnictví, o kterých Navrhovatel tvrdí, že je nezadal.

Finanční arbitr při zkoumání podmínek řízení zjistil, že Navrhovatel a Instituce uzavřeli dne 13. 1. 2005 Smlouvu o sporožirovém účtu (dále jen „Smlouva o sporožirovém účtu"), na základě které Instituce pro Navrhovatele zřídila sporožirový účet č. [redacted] (dále jen „Účet"). Dne 15. 2. 2008 Navrhovatel a Instituce uzavřeli Dohodu o změně Smlouvy o sporožirovém účtu (přechod na Smlouvu o sporožirovém účtu Osobní účet České spořitelny a poskytování souvisejících produktů a služeb), která nahradila Smlouvu o sporožirovém účtu (dále jen „Smlouva o osobním účtu"). Dne 11. 6. 2008 Navrhovatel a Instituce uzavřeli Smlouvu o poskytování služeb Servis 24 (dále jen „Smlouva Servis 24"), na základě které se Instituce zavázala poskytovat Navrhovateli služby přímého bankovnictví.

Dne 20. 2. 2013 Navrhovatel a Instituce uzavřeli Rámcovou smlouvu o finančních službách (dále jen „Rámcová smlouva"), jejímž podpisem současně uzavřeli Smlouvu o účtu č. [redacted] (dále jen „Smlouva o účtu") a Smlouvu o kontokorentním úvěru na Účtu, jež se staly přílohou Rámcové smlouvy. Smlouva o účtu nahradila Smlouvu o osobním účtu a současně podle čl. 4. „SERVIS 24" Smlouvy o účtu platí, že Instituce Navrhovateli poskytuje službu internetového bankovnictví.

Rámcová smlouva je rámcovou smlouvou o platebních službách ve smyslu § 127 odst. 1 písm. a) zákona č. 370/2017 Sb., o platebním styku, ve znění účinném od 13. 1. 2018 (dále jen „nový zákon o platebním styku"), resp. do 12. 1. 2018 byla rámcovou smlouvou ve smyslu § 74 odst. 1 písm. a) zákona č. 284/2009 Sb., o platebním styku, ve znění účinném do 12. 1. 2018 (dále jen „zákon o platebním styku"), neboť se v ní Instituce zavázala pro Navrhovatele provádět platební transakce jednotlivě neurčené, protože podle článku čl. 1 „OTEVŘENÍ A VEDENÍ ÚČTU" Smlouvy o účtu platí, že *„[ú]čet, který povedeme v korunách českých, můžete používat k platbám, výběrům a vkladům."*

Dále, Smlouva o účtu je ode dne 1. 1. 2014 smlouvou o účtu podle § 2662 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník").

Účet, který Instituce pro Navrhovatele vede, je platebním účtem podle § 2 odst. 1 písm. b) nového zákona o platebním styku a téhož ustanovení zákona o platebním styku, neboť slouží k provádění platebních transakcí podle § 2 odst. 1 písm. a) zákona o platebním styku, tj. ke vkladům peněžních prostředků na platební účet, výběrům peněžních prostředků z platebního účtu a převodům peněžních prostředků.

Internetové bankovnictví, prostřednictvím kterého Navrhovatel Účet ovládal, je platebním prostředkem ve smyslu § 2 odst. 1 písm. d) nového zákona o platebním styku a téhož ustanovení 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 zadané prostřednictvím internetového bankovnictví jsou platebními transakcemi podle § 3 odst. 1 písm. c) bodu 3., resp. § 3 odst. 1 písm. d) bodu 3. nového zákona o platebním styku a téhož ustanovení nového zákona o platebním styku (tj. převodem peněžních prostředků z platebního účtu z podnětu plátce).

Finanční arbitr považuje Navrhovatele za spotřebitele podle § 1 odst. 1 zákona o finančním arbitrovi, protože nezjistil, že by Navrhovatel ve smluvním vztahu s Institucí nevystupoval jako fyzická osoba, která nejedná v rámci své obchodní nebo jiné podnikatelské činnosti, jak definují spotřebitele hmotněprávní předpisy.

Instituce je bankou podle zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů (dále jen „zákon o bankách"), tedy osobou oprávněnou mimo jiné poskytovat platební služby. Jelikož finanční arbitr při zkoumání podmínek řízení nezjistil žádné skutečnosti, které by zpochybnily, že Instituce v předmětném smluvním vztahu nevystupuje v postavení poskytovatele platebních služeb, považuje finanční arbitr Instituci za instituci ve smyslu ustanovení § 3 odst. 1 písm. a) zákona o finančním arbitrovi.

K rozhodování sporu mezi Navrhovatelem a Institucí je finanční arbitr příslušný, neboť se jedná o spor mezi spotřebitelem a poskytovatelem platebních služeb při poskytování platebních služeb podle § 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 tvrdí, že *„[s]tal jsem se útokem hackerů, pishingu prostě a jednoduše jsem přes fcb přišel o veškeré mé finanční prostředky na mém účtu, který mám u ČS přes 13 let přesněji 152 tisíc. […] část peněz přesněji 140.000,- si podvodníci poslali na účet taktéž u ČS, […] Zbylých 12 tisíc odešlo na účet u Fio banky."*

Navrhovatel tvrdí, že *„[b]ohužel jsem naletěl podvodníkovi, který se vydával za mého kamaráda na fcb přes masenger, záhadným způsobem přišel k přihlašovacím údajům, které jsem měl uložené jen v mé hlavě, nikde jsem je neměl napsané, nikomu jsem je nesděloval nikdy po telefonu, mazal všechny podezřelé emaily a snažil se dodržovat bezpečnostní základy při užívání servis 24 jakož to běžný uživatel, […] Ihned po zjištění jsem volal a zablokoval svůj účet […] bylo taktéž zjištěno, že jsem se stal obětí již delší dobu známého podvodu přes fcb, kdy i přímo na tento druh upozorňovala moje banka ČS údajně různými upozorněními v podobě informací na bankomatech, zprávami na mém účtu, reklamami aj.“*

Navrhovatel doplňuje, že *„[p]o nainstalování programu, který mi byl zaslán v odkaze od ČS mi tento program zjistil 5 virů, kdy jeden z nich podle mého scanuje přihlašovací údaje, ale expert nejsem. Antivirový program byl stále zapnutý a aktualizovaný. […] Dále se mi paní ombudsmanka snažila podsunout takový závěr, že v minulosti chodily podvodné odkazy na internetové bankovnictví, kdy klient pod záminkou 400 korun vyplnil své přihlašovací údaje do svého servis 24 a tento podvodný odkaz je zkopíroval, ale jsem si zcela jist, že tento email jsem ihned smazal, jelikož jsem si všiml různých nesrovnalostí jako např. špatná čeština, pozměněna hlavička atd. a v žádném případě jsem své údaje do kolonek nevyplňoval. […] servis 24 spravují vice méně přes telefon, kdy upozorňující zprávy nemám šanci zahlédnout […] Na svém účtu jsem v inkriminovanou dobu nebyl přihlášený, žádnou platbu jsem nezadával a ani mě nepřišla autorizační sms na moje nahlášený telefonní číslo.“*

Navrhovatel tvrdí, že *„[p]odle mého názoru spatřuji chybu ze strany Instituce zejména v nedostatečné informovanosti klienta (čili mne) na možná rizika při používání internetového bankovnictví Servis24. Nicméně já, jakožto běžný uživatel, jsem se s takovým upozorněním nesetkal a ani ho nikde neviděl.“*

Navrhovatel namítá, že *„[c]o se týká autorizačních SMS o odvodu peněz z účtu na telefonní číslo klienta, nesetkal jsem se, konkrétně u ČS, s případem, že by SMS obsahovala informaci o tom, z jakého účtu peníze při transakci odcházejí. […] Pokud bych tuto informaci v SMS dostal, prověřil bych si její obsah a poté jednal. […]. Transakce, které odešly z mého účtu, nebyly zadány mojí osobou, tudíž se domnívám, že z tohoto hlediska není vina na mé straně.”*

Navrhovatel tvrdí, že *„telefonní číslo, na které jsem přijal autorizační SMS jé mé soukromé, tj. [redacted] […] způsob poskytnutí autorizační SMS kódu k převodu peněžních prostředků ve výši 12.000 CZK byl identický jako první případ se 140.000 CZK, ale po poskytnutí prvního kódu a přihlášení do Servis24, jsem se zalekl a poslanou SMS s druhým kódem po odeslání jsem okamžitě smazal v domnění, že zabráním dalšímu odcizení peněz, ale ve výpisu, který dokládám, je tento krok zaznamenaný a zvýrazněný […] ohledně odcizení jsem se dozvěděl neprodleně poté, co jsem se přihlásil do Servis24 přes počítač, kde jsem zjistil první a následně i druhou odeslanou transakci.”*

Navrhovatel dále tvrdí, že *„detekci virů jsem nainstaloval do svého počítače, novou instalaci operačního systému jsem na žádost PČR zatím neprováděl, mobilní telefon jsem také, na žádost PČR, do továrního nastavení neuvedl, do internetového bankovnictví jsem nikdy nevstupoval prostřednictvím odkazu na Facebooku. […] Antivirový program v mobilním telefonu je součástí operačního systému a automaticky se aktualizuje se změnou či upgradem telefonu. Tento telefon jsem zakoupil dne 17. 6. 2016 z internetového portálu [redacted]“.*

Navrhovatel dále tvrdí, že *„servis nemohl dohledat historii prohlížeče v mém stolním PC měsíc zpět před odcizenými penězi. Přímo zaměstnankyní ČS […] mi bylo doporučeno, abych při svolení PČR provedl přeinstalaci operačního systému. PČR jsem o tom informoval a vyčkával. PČR veškeré úkony s PC, které potřebovali provést, měla hotové během jednoho dopoledne u mě doma. […] Po úkonech jsem se raději ještě jednou zeptal, zda-li mohu provést přeinstalování systému a taktéž PČR mi toto velmi důrazně doporučila. Řídil jsem se pokyny od pracovnice ČS a systém nechal přeinstalovat.“*

Navrhovatel dále doplnil, že *„Bohužel musím konstatovat, že v celém trestním spise jsem nenašel záznam historie z mého PC a taktéž mobilního telefonu. […] Částku 12.000 Kč jsem neobdržel. Ze spisu jsem pouze vyčetl, že zmíněná částka je zablokovaná policií v jiném členském státě EU."*

Navrhovatel dále tvrdí, že *„IP adresu svého PC neznám ani tak mobilního telefonu, který jsem v té době používal, takže nemohu zcela s jistotou určit, která přihlášení jsem provedl já a která nikoliv […]. Antivirovou kontrolu mobilního telefonu jsem proved na pokyn operátorky ČS, ihned po zjištění odcizených peněz."*

6 Tvrzení Instituce

Instituce potvrzuje, že dne 17. 7 2016 v 16:09:01 hod. přijala platební příkaz k převodu peněžních prostředků ve výši 140.000 Kč z Účtu na účet č. [redacted] z IP adresy [redacted]. Ze stejné IP adresy přijala žádost o vygenerování autorizačního kódu, v 15:56:52 hod. odeslala autorizační zprávu na telefonní číslo [redacted] (dále jen „Telefonní číslo Navrhovatele"); platební příkaz byl autorizačním kódem potvrzen v 16:09:01 hod. z IP adresy [redacted]; peněžní prostředky Instituce odepsala z Účtu téhož dne v 16:09:06 hod. Instituce potvrzuje, že na účet č. [redacted] připsala platbu dne 17. 7. 2016 v 16:09:06 hod. Peněžní prostředky ve výši 140.000 Kč byly z účtu č. [redacted] vybrány v hotovosti dne 17. 7. 2016 v 18:18 hod.

Instituce dále potvrzuje, že téhož dne v 19:46:20 hod. přijala platební příkaz k převodu peněžních prostředků ve výši 12.000 Kč z Účtu na účet č. [redacted] z IP adresy [redacted]. Ze stejné IP adresy přijala žádost o vygenerování autorizačního kódu a v 19.43.56 hod. odeslala autorizační zprávu na Telefonní číslo Navrhovatele; platební příkaz byl autorizačním kódem potvrzen v 19.46.20 hod. z IP adresy [redacted]. Instituce peněžní prostředky z Účtu odepsala dne 18. 7. 2016, 01:17:09 hod. Na účet České národní banky k provedení zúčtování byla platba připsána dne 18. 7. 2016, 05:11:22 hod.

Instituce dále potvrzuje, že téhož dne byla v internetovém bankovnictví Navrhovatele zadána platba ve výši 4.500 Kč z IP adresy [redacted]. Požadavek na zaslání autorizačního kódu byl odeslán ze stejné IP adresy v 18.56.11 hod. Ve stejný čas Instituce odeslala autorizační zprávu na Telefonní číslo Navrhovatele. Protože zadaná platba ve výši 4.500 Kč nebyla autorizačním kódem potvrzena, Instituce tak platební příkaz neprovedla.

Instituce vysvětluje, že *„[v] průběhu dní 16. – 17. 7. 2016 zaznamenala ČS nový druh phisingového útoku, který má podle našich zjištění probíhat tak, že na sociální síti Facebook byl neznámou osobou vytvořen profil pod názvem Servis 24, který pod záminkou vyplacení bonusu 400 Kč lákal na využití nové verze internetového bankovnictví České spořitelny, a.s. s přístupem z falešné webové stránky http://servis24.ic.cz, popřípadě http://sporitelna24_ic_cz nebo http://sporitelnabanking_ic_cz. […] Po rozkliknutí podvodné webové stránky se klientovi nabídne přihlašovací stránka do internetového bankovnictví, která na první pohled vypadá podobně, jako přihlašovací stránka do skutečného internetového bankovnictví SERVIS 24, avšak adresa webu v adresním řádku prohlížeče neodpovídá […]. Poté, co klienti vyplní své přihlašovací údaje do služby SERVIS 24 na těchto podvodných stránkách, získá pachatel přístup do jejich internetového bankovnictví. Následuje kontaktování klienta ze strany pachatele pod profilem klientova přítele na Facebooku, s žádosti o přeposlání autorizačního kódu obsaženého v SMS, kterou si pachatel nechá vygenerovat v rámci zadané transakce v internetovém bankovnictví klienta. […]"*

Instituce namítá, že v případě phishingového útoku na Účet Navrhovatele bylo zjištěno, že *„online scanner ESET, který byl pracovníky Instituce zaslán Navrhovateli k prozkoumání počítače k detekování případných zavirovaných souboru, detekoval přítomnost viru tzv. trojského koně; z Navrhovatelem předložené facebookové komunikace vyplynulo, že tento*

přeposlal autorizační SMS kódy k oběma transakcím pachateli; je dána časová souvislost útoku s výskytem podvodného facebookového profilu a vektor útoku vykazuje znaky výše uvedeného podvodu“ a dovozuje, že Navrhovatel s největší pravděpodobností vyplnil své přihlašovací údaje ke službě SERVIS 24 do podvodných webových stránek, popřípadě, že vir v jeho počítači zpřístupnil pachateli přihlašovací údaje do služby SERVIS 24 nebo své přihlašovací údaje jiným způsobem nezabezpečil a zpřístupnil je třetí osobě, která takto získala přístup do internetového bankovnictví SERVIS 24.

Instituce namítá, že z jejího hlediska *“obě transakce proběhly na základě 3 kroků, kterými jsou zadání klientského čísla a hesla do internetového bankovnictví, které měl k dispozici pouze Navrhovatel a následně vepsání autorizačního kódu, který byl zaslán na sjednané telefonní číslo.“*

Instituce tvrdí, že k blokaci Navrhovatele, včetně blokace služby internetového bankovnictví došlo dne 17. 7. 2016, v 19.50 hod.

Instituce dále vysvětluje, že *„na tzv. neinvazivní zprávu je klient upozorněn červeným kolečkem s číslicí vyjadřující počet nepřečtených zpráv u ikony siluety a obálky v pravém horním rohu domovské stránky po přihlášení do služby SERVIS 24. Po rozkliknutí se zobrazí náhled na seznam zpráv a při jejich otevření získá klient náhled na zprávu ve formě, v jaké mu je zobrazena invazivní zpráva i po přihlášení do služby SERVIS 24.“*

7 Jednání o smíru

Navrhovatel považuje za možné smírné řešení sporu vyplacení 80 % z částky 140.000 Kč a 80 % z částky 12.000 Kč, *„jelikož jsem si vědom i částečného pochybení na mé straně (nedodržení podmínek ve smyslu článku 21.3 a 21.4 Všeobecných obchodních podmínek České spořitelny)“*.

V průběhu řízení finanční arbitr vyzval Instituci, aby ve sporu zvážila částečné smírné řešení, protože Navrhovatel oznámil Instituci zneužití internetového bankovnictví dne 17. 7. 2016 v 19:48:09 hod, tedy ještě před přijetím platebního příkazu k provedení převodu peněžních prostředků ve výši 12.000 Kč z Účtu na účet č. [redacted], který Instituce provedla dne 18. 7. 2016. Instituce dne 19. 7. 2018 zaslala na účet Navrhovatele č. [redacted] částku 12.000 Kč.

Ve zbývající části Instituce možnost smírného řešení sporu odmítla.

8 Právní posouzení

Finanční arbitr podle § 12 odst. 1 a 3 zákona o finančním arbitrovi rozhoduje podle svého nejlepšího vědomí a svědomí, nestranně, spravedlivě a bez průtahů a pouze na základě skutečností zjištěných v souladu se zákonem o finančním arbitrovi a zvláštními právními předpisy. Finanční arbitr při svém rozhodování vychází ze skutkového stavu věci a volně hodnotí shromážděné podklady.

Finanční arbitr rozhoduje podle práva, posuzuje všechny shromážděné podklady samostatně i ve vzájemné souvislosti s přihlédnutím k předmětu projednávaného sporu. Finanční arbitr se tam, kde je to možné, opírá a odvolává na relevantní ustálenou judikaturu obecných soudů nebo Ústavního soudu. Finanční arbitr tak činí proto, aby jeho rozhodnutí bylo věcně a právně správné a přesvědčivé pro obě strany sporu, a zároveň i pro soud, který bude případně na základě žaloby kterékoli strany sporu rozhodnutí finančního arbitra přezkoumávat, rozhodnutí finančního arbitra jako správné potvrdil a žalobu proti němu zamítl.

Navrhovatel vzal svůj návrh na zahájení řízení částečně zpět, a to v částce 12.000 Kč.

Předmětem sporu mezi Navrhovatelem a Institucí zůstává posouzení nároku Navrhovatele na vrácení částky platební transakce 140.000 Kč, resp. uvedení účtu do stavu, v jakém by byl, kdyby Instituce na základě platebního příkazu neodepsala dne 17. 7. 2016 k tíži Účtu částku ve výši 140.000 Kč, který Navrhovatel nezadal ani neautorizoval.

8.1 Skutková zjištění

Finanční arbitr při posouzení věci vycházel z podkladů předložených Institucí, zejména z Přehledu přístupů do internetového bankovnictví, Přehledu odeslaných sms zpráv a otisků z informačního systému Instituce, které mají povahu výstupu z informačního systému sloužících k provozu platebního styku banky. Finanční arbitr tyto podklady v řízeních s obdobným předmětem sporu vždy využívá a považuje je za spolehlivý zdroj relevantních informací.

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

a) v období od 1. 3. 2016 do 17. 7. 2016 došlo k přihlášení do internetového bankovnictví Navrhovatele

   1. z IP adresy [redacted] celkem 26 krát;
   2. z IP adresy začínající [redacted] celkem 50 krát;
   3. z IP adresy začínající [redacted] celkem 3 krát;
   4. z IP adresy [redacted] celkem 1 krát;
   5. z IP adresy [redacted] celkem 1 krát;
   6. z IP adresy [redacted] celkem 1 krát;

b) dne 18. 4. 2016, 02:09:42 hod., došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted], aniž by došlo k zadání platebního příkazu; k odhlášení z internetového bankovnictví Navrhovatele došlo v 02:09:59 hod.; to vyplývá z Přehledu přístupů do internetového bankovnictví;

c) dne 26. 4. 2016, 11:15:06 hod., došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted], aniž by došlo k zadání platebního příkazu; to vyplývá z Přehledu přístupů do internetového bankovnictví;

d) dne 3. 6. 2016, 17:19:20 hod., došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted], aniž by došlo k zadání platebního příkazu; k odhlášení z internetového bankovnictví Navrhovatele došlo v 17:19:30 hod.; to vyplývá z Přehledu přístupů do internetového bankovnictví;

e) dne 17. 7. 2016, 15:29:54 hod., došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted]; při tomto přihlášení došlo mimo jiné k zobrazení seznamu telefonních čísel pro autorizaci platebních transakcí; k odhlášení z internetového bankovnictví Navrhovatele došlo v 15:37:37 hod.; to vyplývá z Přehledu přístupů do internetového bankovnictví a zobrazeného záznamu *„Seznam tel. čísel pro autorizační sms k účtům uživ“* (tj. každý uživatel může mít nastaveno jiné tel. číslo pro autorizaci transakcí a toto je jejich seznam);

f) dne 17. 7. 2016 Navrhovatel zahájil v 15:51 hod. komunikaci prostřednictvím aplikace Messenger s uživatelem označeným jako „Vojta“; to vyplývá z Navrhovatelem předložených otisků obrazovek jeho konverzace s uživatelem „Vojta“ přes aplikaci Messenger a z tvrzení Navrhovatele v Úředním záznamu z 18. 7. 2016: *„15:51“ “Cau [redacted], si tady prosimte?“ ; „Ahoj Vojto jsem v [redacted]“ ; „Ja bych potreboval takovou malickost od tebe“ ; „Jsem jedno ucho☺“ ; „Potrebuji si přeposlat sporeni akorát na můj mobil nikdy neprijde ten kod, tak jestli bych to nemohl zkusit i na tvůj? Kdyby ti to nahodou prislo? Zkousel sem asi 3 cisla a nic“ ; „Jsem s tím ☺“ ; „Super, tak moment Tak ted by mel prijit*

Tak mi ho kdyztak napis sem“ ; „CS-S24: Zadana transakce na ucet [redacted]; castka 140000,00 CZK. Autorizacni SMS kod: [redacted]“ ; „Super tak snad mi to pujde Diky moc Neprisel ještě jeden?“ ; „Ne Vojto“ ; „V pohode Tak kdyby náhodou ještě tak mi napis diky“ „18:57“ „Teď by měl ještě jeden [redacted] jestli to neva“ ; „19:41“ „CS-S24: Transaction set up for account 0-[redacted]; amount 4500,00 CZK. SMS authorization code: [redacted]“ ; „On uz vyprasel cas tak ještě jednou jestli neva“ ; „Nevadi Vojto“; „Díky tak teď by měl přijít Super diky A jak jinak je?“ ; „Vojto? Zmizeli mi peníze z uctu“ ; „Kolik?“; „Vsechno“ ; „Jak všechno?“ ; „Co to je ???? Vojto proboha“ ; „Ja nerozumim“ ; „Volal si do Spořitelny?“ ; „Ano“ ; „A vrátili ti to ?“ ; „vzdyt mi to zmizelo ted resim to Můžeš mi zavolat“ ; „Ja ted nemam mobil To bych si to jinak Neposílal na tebe“ ; „A co to bylo? Mě zmizelo z účtu přes 150 tisíc!!!“ ; Já si přeposilal svoje sporeni ze svého účtu nevim co mas s tim tvym co ti rekla spořitelen?“ ; „A proc me to zmizelo ? To je nějaký poděl ?“ ; „ja nevi, co ti rekla spořitelna?“;

g) dne 17. 7. 2016, 15:55:39 hod., došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted]; při tomto přihlášení došlo k zadání požadavku na zaslání autorizačního sms kódu v 15:56:52 hod. (tj. došlo k zadání platebního příkazu ke Sporné platební transakci); Instituce zaslala v 15:56:52 hod. na Telefonní číslo Navrhovatele autorizační zprávu ve znění *„CS-S24: Zadana transakce na ucet [redacted]; castka 140000,00 CZK. Autorizacni SMS kod:* [redacted]“; platební příkaz byl autorizačním sms kódem potvrzen v 16:09:01 hod.; k odhlášení z internetového bankovnictví Navrhovatele došlo v 16:19:42 hod.; to vyplývá z Přehledu přístupů do internetového bankovnictví a Přehledu odeslaných sms zpráv;

h) Navrhovatel v rámci komunikace zahájené v 15:51 hod. prostřednictvím aplikace Messenger přeposlal zprávu s textem *„CS-S24: Zadana transakce na ucet 0-[redacted]; castka 140000,00 CZK. Autorizacni SMS kod:* [redacted]“ uživateli označenému jako „Vojta“; to vyplývá z Navrhovatelem předložených otisků obrazovek konverzace Navrhovatele s uživatelem „Vojta“ přes aplikaci Messenger;

i) dne 17. 7. 2016, 16:09:06 hod., Instituce odepsala částku Sporné platební transakce z Účtu a současně ji v 16:09:06 hod. připsala na účet č. [redacted] (dále jen „Cílový účet“); to vyplývá z výstupu z informačního systému Instituce „Quick 3270 Secure – Session A – QUICK_Pattern_SSL.ecf“ s detaily transakce ze dne 17. 7. 2016 na částku 140.000 Kč a Detailu Sporné platební transakce;

j) dne 17. 7. 2016, 18:18 hod., byla částka Sporné platební transakce z Cílového účtu vybrána v hotovosti; to vyplývá z Detailu Sporné platební transakce a Pokladního dokladu o výběru částky 140.000 Kč z účtu č. [redacted] (Cílový účet) dne 17. 7. 2016 v 18:18 hod.;

k) dne 17. 7. 2016, 18:55:41 hod., došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted]; při tomto přihlášení došlo k zadání požadavku na zaslání autorizačního sms kódu v 18:56:11 hod. (tj. došlo k zadání platebního příkazu); Instituce zaslala v 18:56:11 hod. na Telefonní číslo Navrhovatele autorizační zprávu ve znění *„CS-S24: Transaction set up for account [redacted]; amount 4500,00 CZK. SMS authorization code:* [redacted]“; platební příkaz nebyl autorizačním kódem potvrzen;

l) dne 17. 7. 2016, 18:57 hod. obdržel Navrhovatel v rámci konverzace Navrhovatele s uživatelem označeným jako „Vojta“ přes aplikaci Messenger zprávu „*Teď by měl ještě jeden [redacted] jestli to neva“*; a Navrhovatel v 19:41 hod. přeposlal zprávu s *„CS-S24: Transaction set up for account [redacted]; amount 4500,00 CZK. SMS authorization code:* [redacted]“; Navrhovatel obdržel odpověď *„On uz vyprsel cas“*, *„Tak ještě jednou jestli neva“*; to vyplývá z Navrhovatelem předložených otisků obrazovek konverzace Navrhovatele s uživatelem „Vojta“ přes aplikaci Messenger;

m) dne 17. 7. 2016, 19:43:27 hod., došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adresy [redacted]; při tomto přihlášení došlo k zadání požadavku na zaslání

autorizačního sms kódu v 19:43:56 hod. (tj. došlo k zadání platebního příkazu k platební transakci na částku 12.000 Kč); Instituce zaslala v 19:43:56 hod. na Telefonní číslo Navrhovatele autorizační zprávu ve znění *„CS-S24: Transaction set up for account 0-* [redacted]*; amount 12000,00 CZK. SMS authorization code:* [redacted]*“*; platební příkaz byl autorizačním kódem potvrzen v 19:46:20 hod.; to vyplývá z Přehledu přístupů do internetového bankovnictví a Přehledu odeslaných sms zpráv;

n) Navrhovatel v Úředním záznamu z 18. 7. 2016 tvrdí, že *„[…] vzápětí přišla další autorizační sms přesně v 19:43 hod, tu jsem mu přeposlal […].“;*

o) dne 17. 7. 2016, 19:45:01 hod., došlo k přihlášení do internetového bankovnictví z IP adresy [redacted]; které provedl Navrhovatel, který potvrzuje, že při tomto přihlášení do internetového bankovnictví zjistil provedení Sporné platební transakce; to vyplývá z Přehledu přístupů do internetového bankovnictví, výpisu z Účtu za měsíc červenec 2016 a tvrzení Navrhovatele v Úředním záznamu z 18. 7. 2016 *„[m]ě už pak ale něco říkalo, koukni se na svůj účet, tak jsem se na něj kouknul přes telefon a zjistil, že mě z účtu odešlo 140.000,- Kč.“*;

p) dne 17. 7. 2016, 19:48:09 hod., Navrhovatel telefonicky kontaktoval Instituci; v průběhu telefonního hovoru Instituce zablokovala internetové bankovnictví Navrhovatele, *„Dobrý den, já bych potřeboval ihned zablokovat účet, mě se asi na něj někdo dostal a zmizely mi v něm peníze.“*; to vyplývá ze záznamu telefonního hovoru mezi Instituci a Navrhovatelem [redacted];

q) dne 17. 7. 2016 v 19:50 hod. Instituce zablokovala internetové bankovnictví Navrhovatele, to vyplývá z Přehledu přístupů do internetového bankovnictví („CBL_USR_Lock“ „zablokování uživatele“);

r) v telefonním hovoru mezi Navrhovatelem a Instituci dne 17. 7. 2016 zahájeném v 20:02 hod. Instituce Navrhovateli sdělila, že *„Každopádně mi to budeme řešit ihned s kolegy z bezpečnostního monitoringu. Podíváme se, zda je možné ten cílový účet nějakým způsobem zablokovat a samozřejmě to řešíme s nejvyšší prioritou. […] Každopádně uděláme všechno, aby bylo možné peníze získat zpět.“;* to vyplývá ze záznamu telefonního hovoru mezi Instituci a Navrhovatelem [redacted];

s) Instituce zaslala dne 17. 7. 2016 v 20:53 hod. prostřednictvím zprávy elektronické pošty Navrhovateli online scanner od antivirové firmy ESET; to vyplývá z e-mailu Instituce odeslaného Navrhovateli dne 17. 7. 2016 v 20:53 hod. s předmětem: „[redacted]“; *„Dobrý den, na základě naší telefonické domluvy Vám zasílám online scanner od antivirové firmy ESET. Jedná se o jednorázový softwarový nástroj, který nechrání počítač před infikováním, ale provede jednorázovou kontrolu počítače aktualizovaným antivirovým programem. […] Znovu připomínáme, že je nutné nechat počítač i telefon ve stávajícím stavu, až po nahlášení celé situace na Policii ČR Vám sdělí, zda budou potřebovat oba přístroje k dalšímu šetření, nebo je můžete „Vyčistit“ popř. přenastavit do továrního nastavení.“;*

t) Antivirový program Online Scanner ESET detekoval v počítači Navrhovatele virus „HackTool:Win32/Keygen“ označovaný jako trojský kůň; to vyplývá ze 7 příloh s výsledky antivirového programu, které Navrhovatel zaslal Instituci dne 18. 7. 2016 v 15:54 hod. prostřednictvím zprávy elektronické pošty, kterou předložila Instituce;

u) Antivirový program Online Scanner ESET detekoval v počítači Navrhovatele viry označené „Cíl „C:\InstalMicrosoft Toolkit 2.5 2 Cle“ Infiltrace „varianta infiltrace Generik IQFCZZB trojský kůň; Cíl „F:\Borde..bsplayer 264 1073 exe“ Infiltrace „Win32/Toolbar Condu..AE potencionálně nechtěna a“; Cíl „F:\Borde..3d closer to the edge2“ Infiltrace „Win32\InstallMonetizer AF potencionálně nechtěná a“; Cíl „F:\Instal (90% na Vistu)\BitLord_1“ Infiltrace „varianta infiltrace WIn32/Toolbar Condict AR pot“; Cíl „F:\Instal

(90% na Vistu)\Nod 32 .“ Infiltarce „WIN32\RiskWare HackAV BG aplikace“; to vyplývá z fotografie otisku obrazovky s názvem „ESET Online Scanner“ „Výsledek kontroly“ s označenými nalezenými 5 viry předložené Navrhovatelem;

v) Navrhovatel v Úředním záznamu ze dne 18. 7. 2016 oznámil, že *„[v]čera okolo 15:45-15:51 me na aplikaci messenger facebooku přišla zpráva na můj telefon, „Xaoimi redminton 3“ pro (*[redacted]*), od kamaráda […]. V tu chvíli mi přišla sms, která se tvářila jako autorizační, tu jsem zkopíroval a přes messenger jsem mu ji poslal zpátky […] Pak mě od něj přišla další zpráva v 18:57 hod […] a zhruba po hodině mě od něj přišla další autorizační sms, na kterou jsem reagoval až zhruba po hodině, protože telefon jsem neměl u sebe, takže jsem mu tu zprávu přeposlal, ale pozbyla platnost […] vzápětí přišla další autorizační sms přesně v 19:43 hod, tu jsem mu přeposlal […] Mě už pak ale něco říkalo, koukni se na svůj účet, tak jsem se na něj kouknul přes telefon a zjistil jsem, že mě z účtu odešlo 140.000 Kč. […] Ještě uvádím, že nedávno asi tak před 4 až 5 měsíců mě přišlo jakoby od České spořitelny odkaz, a když jsem kliknul tak stránka servisu 24, ale protože na to Česká spořitelna poukazovala, že jde o podvod, tak jsem to nevyplňoval a smazal jsem to.“;*

w) Navrhovatel v Úředním záznamu ze dne 19. 7. 2016 oznámil, že *„[d]ále také poskytuji policii svůj mobilní telefon XIAOMI RED MI NOTE 3 PRO, pro provedení kopie jeho obsahu, resp. provedení bitové kopie pro jeho zkoumání. […] K věci dále uvádím, že policejním orgánu zítra předvedu svůj počítač, který mám doma pro zjištění škodlivého software, případně logu antivirového programu. […]“;*

x) Navrhovatel v Úředním záznamu ze dne 25. 8. 2016 oznámil, že *„[j]e to asi 4 měsíce, kdy mi do mailu […] přišel odkaz servis24, kdy nabízeli 400 Kč jako odměnu pro věrného klienta banky. Klik jsem na odkaz a to v internetovém prohlížeči telefonu, kdy jsem byl přesměrován na přihlašovací stránku servis24, kdy po mě byly požadovány přístupová hesla, vzhledem ke skutečnosti, že stránka servis24 vykazovala gramatické chyby, byla snad i v angličtině, tak jsem tuto stránku uzavřel a e-mail smazal. Žádné přístupové údaje do servis24 jsem zde nevyplnil. […]. K věci dále uvádím, že pro finančního arbitra mám zajištěnou historii prohlížeče jak mobilního telefonu, tak i počítače a to v době jednoho měsíce před samotným útokem, kdy toto doložím do 5. 9. 2016, zároveň předložím policii svůj mobil a počítač za účelem zjištění historie prohlížeče.“*

Finanční arbitr dále ze shromážděných podkladů zjistil, že

(i) Navrhovatel si v internetovém bankovnictví zobrazil zprávy Instituce: dne 4. 4. 2014 v 10:07 hod. *„Upozorňujeme na nové chování počítačového viru“*, dne 11. 6. 2014 v 19:42 hod. *„Jak se bezpečně chovat na internetu“*, dne 9. 9. 2014 v 14:11 hod. *„Aktivovali jsme vám bezpečnější platbu kartou na internetu se službou 3D Secure“*, dne 21. 12. 2014 v 12:56 hod. *„Upozornění na podvody přes Facebook“*, dne 9. 4. 2015 v 18:09 hod. *„Upozornění na nové chování počítačového viru“*, dne 10. 4. 2015 v 15:05 hod. *„Chraňte se před podvodníky v internetovém světě“*, dne 27. 7. 2015 v 11:44 hod. *„POZOR! Nenechte se na Facebooku okrást!“*, dne 9. 9. 2015 v 18:30 hod. *„Upozornění na nový phisingový útok“*; to vyplývá z Přehledu přístupů do internetového bankovnictví „Zobrazení bankovní zprávy“ a z otisku obrazovek bezpečnostních upozornění;

(ii) Navrhovatel si dne 29. 10. 2015 v 14:21 hod. v internetovém bankovnictví zobrazil zprávu Instituce *„Upozornění na možné zneužití internetového bankovnictví prostřednictvím Facebooku“*, která mimo jiné obsahovala upozornění *„Podvodník osloví klienta pod profilem někoho z jeho přátel o zaslání nějakého finančního obnosu (obvykle ve výši 30 až 50 Kč). […] Aby se podvodník dostal k potvrzovací SMS zprávě, sdělí klientovi, že má nějaký problém s telefonem, a požádá, jestli si může nechat poslat autorizační sms na telefon klienta s tím, aby mu ji klient následně přeposlal. […] Upozorňujeme, abyste na*

podobné zprávy v žádném případě nereagovali a nezadávali požadované údaje. […] Přihlašovací údaje k internetovému bankovnictví je nutné bedlivě hlídat a chránit před vyzrazením. Proto nikdy nedejte na jakkoli úpěnlivé výzvy, podoba podvodu se může časem změnit. […] Nikdy také nepřeposílejte žádné své autorizační SMS zprávy další osobě.“; to vyplývá z otisku obrazovky s bezpečnostním upozorněním č. [redacted], z Přehledu přístupů do internetového bankovnictví „Zobrazení bankovní zprávy“.

Navrhovatel na druhou stranu nepředložil, ačkoli ho k tomu v průběhu řízení finanční arbitr vyzval:

a) přehled internetové historie počítače, ze kterého Navrhovatel před provedením Sporné platební transakce do internetového bankovnictví přistupoval; Navrhovatel předložil dva soubory ve formátu prostého textu, z nichž jeden označil za historii prohlížeče za měsíc červen a druhý za měsíc červenec 2016, ze kterých však nebyly patrné data a časy navštívení jednotlivých webových stránek; Navrhovatel finančnímu arbitrovi sdělil, že historii z počítače musí provést specializovaná firma, protože sám to neumí, a následně, že servis nemohl dohledat historii prohlížeče v počítači, protože se řídil pokyny pracovnice Instituce a systém nechal přeinstalovat;

b) přehled internetové historie mobilního telefonu Navrhovatele za dobu jednoho měsíce před provedením Sporné platební transakce; Navrhovatel předložil historii za období od 20. 6. 2016 do 5. 7. 2016 a následně sdělil, že historii z mobilního telefonu musí provést specializovaná firma, protože sám to neumí, a poté předložil Servisní protokol, ze kterého vyplývá, že z telefonního přístroje značky „Cubot X 11“, „seriové číslo [redacted]“ nelze vyjmou data z historie prohlížeče za období od 17. 6. 2016 do 17. 7. 2016;

c) doklad o tom, že počítač, ze kterého přistupoval do internetového bankovnictví, byl před provedením Sporné platební transakce chráněn antivirovým programem Windows Defender, když Navrhovatel předložil otisk obrazovky označené Název položky „Microsoft Security Essentials.lnk“, Typ „Zástupce“, Cesta ke složce „C:\ProgramData\Microsoft\Windows\nabídky…“, Datum vytvoření „6. 12. 2015 21:23“, Datum změny „6. 12. 2015 21:23“;

d) doklad o tom, že jeho mobilní telefon, byl před provedením Sporné platební transakce chráněn integrovaným antivirovým programem, když Navrhovatel pouze sdělil *„Antivirový program v mobilním telefonu je součástí operačního systému a automaticky se aktualizuje se změnou či upgradem telefonu.“*;

e) v přehledu přihlášení do internetového bankovnictví Navrhovatele označení přihlášení, která provedl Navrhovatel, a to jak ze svého počítače, tak ze svého mobilního telefonu; Navrhovatel sdělil, že IP adresu svého PC a mobilního telefonu nezná a nemůže tak s jistotou určit, která přihlášení provedl a která nikoliv.

8.2 *Rozhodná právní úprava*

Protože k rozhodným skutkovým okolnostem došlo před nabytím účinnosti nového zákona o platebním styku, tedy před 13. 1. 2018, rozhodnou právní úpravu netvoří nový zákon o platebním styku, ale zákon o platebním styku, protože podle § 275 nového zákona o platebním styku, platí, že *„[z]ávazek ze smlouvy o platebních službách se řídí tímto zákonem ode dne nabytí účinnosti, i když k uzavření smlouvy o platebních službách došlo před tímto dnem; vznik této smlouvy, jakož i práva a povinnosti z ní vzniklé přede dnem nabytí účinnosti tohoto zákona se však posuzuje podle zákona č. 284/2009 Sb., ve znění účinném přede dnem nabytí účinnosti tohoto zákona“.*

Na právní vztahy mezi Navrhovatelem a Institucí z Rámcové smlouvy se dále použije úprava občanského zákoníku. Zákon o platebním styku je pak ve vztahu k občanskému zákoníku

právním předpisem speciálním, pokud tedy zákon o platebním styku neupravuje určitou otázku, použije se občanský zákoník jako obecný soukromoprávní předpis.

8.3 Rozhodná smluvní úprava

Dne 20. 2. 2013 Navrhovatel a Instituce uzavřeli Rámcovou smlouvu, jejímž podpisem současně uzavřeli Smlouvu o účtu, která nahradila Smlouvu o osobním účtu, neboť podle čl. 1 „OTEVŘENÍ A VEDENÍ ÚČTU“ Smlouvy o účtu platí, že *„[n]a základě dříve uzavřené smlouvy Vám vedeme účet č. [redacted]. Tato dříve uzavřená smlouva bude nahrazena touto smlouvou, která současně zruší a nahradí i veškerá další ujednání týkající se poskytování služeb k uvedenému účtu, pokud v této smlouvě nedohodneme jinak. […] Podrobné podmínky pro vedení účtu a jeho používání najdete ve Všeobecných obchodních podmínkách České spořitelny, a.s., a ve sdělení k platebním službám a účtům“.*

Současně podle čl. 4. „SERVIS 24“ Smlouvy o účtu platí, že Instituce Navrhovateli poskytuje službu internetového bankovnictví, neboť *„[t]oto ujednání o využívání služeb SERVIS 24 nahrazuje Vaši dříve uzavřenou smlouvu o přímém bankovnictví. Nadále však zůstávají zachovány dosavadní bezpečnostní a přihlašovací údaje ke službám SERVIS 24 (pokud zároveň nežádáte o jejich znovuvytvoření), adresa pro zaslání bezpečnostních údajů ke službám SERVIS 24 (pokud zároveň nežádáte o její změnu), všechna Vámi provedená nastavení služeb SERVIS 24 a dále veškerá ujednání, která se týkají připodepisování všech plateb prováděných prostřednictvím služeb SERVIS 24, využívání vyššího typu zabezpečení a zmocněných osob. Podrobné podmínky pro zřízení a využívání služeb SERVIS 24 najdete ve Všeobecných obchodních podmínkách České spořitelny, a.s., a příručce služeb SERVIS 24. Bezpečnostní limity pro platby prováděné prostřednictvím služeb SERVIS 24 najdete ve sdělení k platebním službám a účtům. Bereme na vědomí Vaše rozhodnutí, že pro účely služeb SERVIS 24 bude Váš účet sloužit jako primární účet“.*

Podle čl. 8 „ZÁVĚREČNÁ USTANOVENÍ“ Smlouvy o účtu platí, že *„[p]odmínky výslovně v této smlouvě neupravené se řídí Všeobecnými obchodními podmínkami České spořitelny, a.s. Podpisem této smlouvy potvrzujete, že jste Všeobecné obchodní podmínky České spořitelny, a.s., a další dokumenty, na které tato smlouva odkazuje převzal(a), že jste se s jejich obsahem seznámil(a) a že s nimi souhlasíte“.*

Smlouva o účtu tak označuje ve svém čl. 8 „ZÁVĚREČNÁ USTANOVENÍ“ za svou nedílnou součást Všeobecné obchodní podmínky České spořitelny, a.s., v tomto případě účinné od 1. 4. 2011 (dále jen „Všeobecné podmínky“).

Dále podle čl. 8 „ZÁVĚREČNÁ USTANOVENÍ“ Smlouvy o účtu se nedílnou součástí Smlouvy o účtu, stala Uživatelská příručka služeb SERVIS 24, v tomto případě ve verzi „9/2012“ (dále jen „Příručka služeb SERVIS 24“) a Sdělení k platebním službám a účtům Soukromá klientela, v tomto případě účinné ode dne 10. 1. 2013 (dále jen „Sdělení k platebním službám“).

Finanční arbitr v řízení vyzval Instituci, aby sdělila, zda za trvání smluvního vztahu mezi Navrhovatelem a Institucí došlo ke změnám Rámcové smlouvy, a pokud ano, aby doložila, že ke změně došlo v souladu s Rámcovou smlouvou a v souladu s právními předpisy; tedy zejména v souladu se zákonem o platebním styku, který v § 94 stanoví, že *„[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 § 94 odst. 3 písm. d) zákona o platebním styku *„[b]ylo-li to dohodnuto, platí, že uživatel návrh na změnu závazku z rámcové smlouvy přijal, jestliže poskytovatel v návrhu na změnu závazku z rámcové smlouvy informoval uživatele o jeho právu vypovědět závazek z rámcové smlouvy podle odstavce 4“* a podle § 94 odst. 4 platí, že *„[j]estliže uživatel návrh na změnu závazku z rámcové smlouvy v případě uvedeném v odstavci 3 odmítne, má právo závazek z rámcové smlouvy přede*

dnem, kdy má změna nabýt účinnosti, bezúplatně a s okamžitou účinností vypovědět“. Trvalým nosičem dat je podle § 2 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“*.

Instituce předložila Všeobecné obchodní podmínky České spořitelny, a.s. účinné ode dne 1. 1. 2014 a Všeobecné obchodní podmínky České spořitelny, a.s. účinné ode dne 1. 7. 2016, avšak nedoložila, že se tyto podmínky staly součástí Smlouvy o účtu v souladu s § 94 zákona o platebním styku, a to s přihlédnutím k rozhodnutí Evropského soudního dvora ve věci BAWAG.

Instituce dále předložila Příručku služeb SERVIS 24 a Sdělení k platebním službám, které finanční arbitr považuje podle čl. 8 „ZÁVĚREČNÁ USTANOVENÍ“ Smlouvy o účtu za nedílnou součástí Smlouvy o účtu.

Finanční arbitr tak jako smluvní úpravu rozhodnou pro posouzení tohoto případu považuje mimo Smlouvy o účtu, Všeobecné podmínky (tedy Všeobecné obchodní podmínky České spořitelny, a.s. účinné ode dne 1. 4. 2011), Příručku služeb SERVIS 24 (tedy Uživatelskou příručku služeb SERVIS 24 ve verzi „09/2012“) a Sdělení k platebním službám (tedy Sdělení k platebním službám a účtům Soukromá klientela účinné ode dne 10. 1. 2013).

8.4 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 převody peněžních prostředků, jsou podle § 98 odst. 1 zákona o platebním styku autorizovány, 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 ve Všeobecných podmínkách a Příručce služeb SERVIS 24.

Podle článku 31.6 Všeobecných podmínek „Souhlas s provedením platební transakce“ *„[b]anka provede pouze takovou platební transakci, s jejímž provedením vyslovil Klient souhlas před předáním platebního příkazu a nejpozději společně s jeho doručením. Taková platební transakce je autorizovanou platební transakcí. […] Udělení Klientova souhlasu k platební transakci je podmínkou jejího provedení.“* Podle článku 31.6 „Souhlas s provedením platební transakce“ písm. b) Všeobecných podmínek *„[j]e-li platební příkaz pořízen za využití některé služby přímého bankovnictví, pak použitím popřípadě sdělením Bezpečnostních údajů, společně s řádnou identifikací jednajícího Uživatele, případně i použitím Bezpečnostních prostředků, při pořízení a předání platebního příkazu Bance, Klient vyjadřuje svůj souhlas s provedením platební transakce na základě takového platebního příkazu“.*

Podle článku 4. „Přihlášení do služeb SERVIS 24“ Příručky služeb SERVIS 24 je využití služeb internetového bankovnictví SERVIS 24 *„[p]odmíněno úspěšným přihlášením, které slouží k identifikaci a ověření uživatele“*.

Článek 4.2 „Přihlášení do služby SERVIS 24 Internetbanking“, „Druhé a další přihlášení“ Příručky služeb SERVIS 24 stanoví: *„[k] přihlášení použijte klientské číslo a aktuální heslo pro Internetbanking, případně také přihlašovací SMS kód“.*

Podle článku 3. „Bezpečnost služeb SERVIS 24“ Příručky služeb SERVIS 24 je přihlašovací sms volitelně nastavitelným bezpečnostním údajem. Finanční arbitr ze shromážděných podkladů nezjistil, že by si Navrhovatel nastavil přihlašovací sms kód jako jeden z bezpečnostních údajů pro přihlášení do internetového bankovnictví.

Článek 3.1 „Poskytování bezpečnostních údajů“ Příručky služeb SERVIS 24 stanoví, že *„[p]ro zadávání aktivních transakcí prostřednictvím služby SERVIS 24 Internetbanking je nutné ke standardní bezpečnosti aktivovat autorizační SMS“.*

Podle článku 3.2 „Identifikace a ověření uživatele“ Příručky služeb SERVIS 24 je autorizační sms *„SMS, kterou zasílá banka uživateli na jeho mobilní telefon, a která obsahuje autorizační SMS kód. Autorizační SMS kód slouží k autorizaci transakcí pořizovaných uživatelem prostřednictvím služby SERVIS 24 Internetbanking. Během autorizace je třeba SMS kód opsat z SMS zprávy do příslušného pole v aplikaci Internetbanking. […]“.*

Navrhovatel si tedy s Institucí sjednal, že souhlas s platební transakcí zadanou prostřednictvím internetového bankovnictví uděluje tak, že se do internetového bankovnictví přihlásí pomocí klientského čísla a hesla pro Internetbanking a zadaný platební příkaz potvrdí zadáním autorizačního sms kódu zaslaného na Telefonní číslo Navrhovatele do příslušného pole.

Z Přehledu přístupu do internetového bankovnictví a Přehledu odeslaných sms zpráv finanční arbitr zjistil, že Sporná platební transakce byla provedena po úspěšném přihlášení do internetového bankovnictví Navrhovatele a za použití autorizačního sms kódu. Finanční arbitr uzavírá, že předloženými podklady Instituce doložila, že při Sporné platební transakci byla dodržena sjednaná forma a postup.

8.5 Sporná platební transakce jako neautorizovaná platební transakce

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.

Právní úprava obsažená v ustanoveních § 98 a § 120 zákona o platebním styku vychází ze Směrnice. Čl. 59 odst. 2. Směrnice v tomto směru přitom vymezuje, 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.“*

Přestože tedy zákon o platebním styku neobsahuje jako v jiných případech doslovnou transpozici, pořád platí, že podle zásad, které platí jak v civilním soudním řízení, tak v řízení před finančním arbitrem, je finanční arbitr povinen vycházet ze skutkového stavu věci a volně hodnotit shromážděné důkazy (k tomu srov. Beran, J., Doležalová, D., Strnadel, D., Štěpánová, A.: Zákon o platebním styku. Komentář. 1. vydání. Praha: C. H. Beck, 2011).

Navrhovatel tvrdí, že Spornou platební transakci nezadal a že tuto platební transakci neautorizoval.

Z Přehledu přístupů do internetového bankovnictví a Přehledu odeslaných sms zpráv vyplývá, že Sporná platební transakce byla provedena po úspěšném přihlášení do internetového bankovnictví Navrhovatele a za použití autorizačního sms kódu.

Protože skutkové okolnosti případu, vyplývající zejména z konverzace Navrhovatele s uživatelem označeným jako „Vojta“ přes aplikaci Messenger a z Úředních záznamů z 18. 7. 2016, 19. 7. 2016 a 25. 8. 2016, nasvědčují tomu, že Navrhovatel platební příkaz ke Sporné platební transakci skutečně nezadal, posuzuje finanční arbitr Spornou platební transakci jako platební transakci neautorizovanou, se kterou zákon o platebním styku spojuje právní následky v podobě speciální odpovědnosti poskytovatele nebo uživatele platebních služeb za neautorizovanou platební transakci.

8.6 Odpovědnost za Spornou platební transakci jako 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 internetového bankovnictví Navrhovatele, 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.“*

8.7 Oznámení zneužití platebního prostředku

Prostředkem umožňujícím oznámit zneužití internetového bankovnictví je podle článku 24.4 „Ztráta, odcizení nebo zneužití Bezpečnostních údajů nebo Bezpečnostních prostředků“ Všeobecných podmínek informační linka Instituce nebo telefonní čísla uvedená v dalších informačních materiálech Instituce.

Z vyjádření obou stran sporu ani z podkladů shromážděných finančním arbitrem nevyplynulo, že by tyto linky nebyly v rozhodné době pro tento případ v provozu nebo že by se Navrhovatel pokusil kontaktovat Instituci dříve a nepodařilo se mu to.

Ze shromážděných podkladů a doložených tvrzení stran sporu vyplývá, že

1. platební příkaz ke Sporné platební transakci byl zadán dne 17. 7. 2016 v 15:56:52 hod. a potvrzen zadáním autorizačního sms kódu v 16:09:01 hod.;
2. Instituce Spornou platební transakci odepsala z Účtu dne 17. 7. 2016 v 16:09:06 hod.;
3. Instituce částku Sporné platební transakce připsala na Cílový účet v 16:09:06 hod.;
4. částka Sporné platební transakce byla z Cílového účtu vybrána dne 17. 7. 2016 v 18:18 hod.;
5. Navrhovatel dne 17. 7. 2016 v 19:48:09 hod. kontaktoval telefonicky Instituci a v 19:50 hod. Instituce zablokovala internetové bankovnictví Navrhovatele.

Navrhovatel oznámil zneužití internetového bankovnictví až po provedení Sporné platební transakce a použití ustanovení § 116 odst. 2 zákona o platebním styku tedy v případě Sporné platební transakce nepřichází v úvahu.

8.8 Ochrana personalizovaných bezpečnostních prvků

Ze shromážděných podkladů vyplývá, že Sporná platební transakce byla provedena s použitím klientského čísla a hesla pro Internetbanking pro přihlášení do internetového bankovnictví Navrhovatele a autorizačního sms kódu k Sporné platební transakci.

Klientské číslo, heslo pro Internetbanking 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 článku 3.2 „Identifikace a ověření uživatele“ Příručky služeb SERVIS 24 jsou klientské číslo, heslo pro Internetbanking a autorizační sms kód tzv. „Bezpečnostními údaji“.

Podle článku 23.7 „Uživatel služeb přímého bankovnictví“ Všeobecných podmínek *„[b]anka přidělí každému Uživateli Bezpečnostní údaje, případně Bezpečnostní prostředky, které slouží k jeho identifikaci a autentizaci při využití služeb přímého bankovnictví.“*

Podle článku 1.3 „Charakteristika služby SERVIS 24 Internetbanking“ Příručky služeb SERVIS 24 *„[s]lužba SERVIS 24 Internetbanking slouží k obsluze účtů přes internet a je poskytována prostřednictvím internetové aplikace. Zadáním adresy www.servis24.cz do internetového prohlížeče se Vám zobrazí stránky internetového bankovnictví.“*

Článek 4.2 „Přihlášení do služby SERVIS 24 Internetbanking“, „Druhé a další přihlášení“ Příručky služeb SERVIS 24 stanoví: *„[k] přihlášení použijte klientské číslo a aktuální heslo pro Internetbanking, […].“*

Podle článku 3.2 „Identifikace a ověření uživatele“ Příručky služeb SERVIS 24 je klientské číslo *„[d]esetimístné číslo, které jste obdrželi v doporučené zásilce a které při přihlašování slouží k ověření Vaší totožnosti.“*

Podle článku 3.2 „Identifikace a ověření uživatele“ Příručky služeb SERVIS 24 heslo pro Internetbanking *„[s]i stanovíte při prvním přihlášení do služby SERVIS 24 Internetbanking.“*

Podle článku 3.2 „Identifikace a ověření uživatele“ Příručky služeb SERVIS 24 autorizační SMS *„[z]asílá banka uživateli na jeho mobilní telefon, a která obsahuje autorizační SMS kód. Autorizační SMS kód slouží k autorizaci transakcí pořizovaných uživatelem prostřednictvím služby SERVIS 24 Internetbanking. Během autorizace je třeba SMS kód opsat ze SMS zprávy do příslušného pole v aplikaci Internetbanking.“*

V článku 3.2 „Důležité upozornění“ Příručky služeb SERVIS 24 pak Instituce upozorňuje, že *„[p]rozrazením výše uvedených bezpečnostních prvků můžete ohrozit bezpečnost svých účtů obsluhovaných službami SERVIS24. […].”*

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.“* Ze shromážděných podkladů finanční arbitr nezjistil, že by Instituce splnění povinnosti podle § 102 odst. 1 písm. a) zákona o platebním styku 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.“*

Finanční arbitr má za to, že ke zneužití internetového bankovnictví Navrhovatele muselo dojít ve sféře Navrhovatele, a to jednak napadením jeho elektronických zařízení, na kterých Navrhovatel používal internetové bankovnictví ve spojení s tím, že třetí osoba, která získala přístupové údaje do internetového bankovnictví Navrhovatele, si od něj vyžádala autorizační sms kód, který ji Navrhovatel opakovaně sám aktivně přeposlal, a třetí osoba pak prostřednictvím autorizační sms kódu autorizovala Spornou platební transakci.

Finanční arbitr sice nezjistil, kdy a jakým konkrétním způsobem došlo k vyzrazení přístupových údajů do internetového bankovnictví Navrhovatele, ale ze shromážděných podkladů lze s vysokou mírou pravděpodobnosti dovodit, že se tak stalo na straně Navrhovatele.

V počítači Navrhovatele bylo detekováno 5 virů, mezi nimi i virus HackTool:Win32/Keygen, není tedy vyloučeno, aby některý z virů nalezených v počítači Navrhovatele, nemohl potencionálně získat přihlašovací údaje do jeho internetového bankovnictví.

Přestože Navrhovatel tvrdí, že do internetového bankovnictví se přihlašuje přes telefon (*„servis 24 spravují vice méně přes telefon“),* z Navrhovatelem předložené Historie telefonu od 20. 6. 2016 do 5. 7. 2016 finanční arbitr nezjistil, že by se Navrhovatel v tomto období do internetového bankovnictví Instituce přihlásil prostřednictvím tohoto mobilního telefonu, když předložený výpis neobsahuje žádné údaje o zobrazení webových stránek Instituce (http://www.csas.cz) anebo internetového bankovnictví Instituce (http://www.servis24.cz). Protože z Přehledu přístupu do internetového bankovnictví vyplývá, že v tomto období došlo k osmi přihlášením do internetového bankovnictví Navrhovatele, ale Navrhovatel přes výzvu finančního arbitra neoznačil IP adresy, ze kterých se do svého internetového bankovnictví přihlašoval, nemůže finanční arbitr vyloučit, že k získání přihlašovacích údajů do internetového bankovnictví Navrhovatele došlo právě na zavirovaném počítači Navrhovatele, který Navrhovatel také používal k přihlášení do internetového bankovnictví.

Zároveň historii telefonu od 20. 6. 2016 do 5. 7. 2016, kterou předložil Navrhovatel, nelze s jistotou spojit s historií mobilního telefonu, který Navrhovatel používal k přístupu do internetového bankovnictví, protože jediným společným znakem je pouze označení typu

mobilního telefonu ve sloupci „Source“ „Xiaomi_Redmi Note 2.zip/apps/com.android.browser/db/browser2.db“.

Současně sám Navrhovatel nepopírá, *že* v minulosti obdržel e-mail s podvodným odkazem na internetové bankovnictví Instituce, kdy klient pod záminkou obdržení 400 korun vyplnil své přihlašovací údaje do svého Servis24, o kterém Navrhovatel tvrdí, že jej smazal a přihlašovací údaje nezadal, ale své tvrzení nijak nedoložil.

Finanční arbitr současně zjistil, že již dne 18. 4. 2016, 26. 4. 2016 a 3. 6. 2016 došlo k přihlášení do internetového bankovnictví Navrhovatele z IP adres [redacted] (…), které se od IP adresy, ze které došlo k zadání Sporné platební transakce, liší jen v posledním trojčíslí. Protože Navrhovatel přes výzvy finančního arbitra neoznačil IP adresy, ze kterých se do internetového bankovnictví přihlašoval, nemůže finanční arbitr vyloučit, že se již v těchto případech nejednalo o přihlášení třetí osoby, odlišné od Navrhovatele, protože tyto IP adresy se výrazně shodují s IP adresou, ze které došlo k provedení Sporné platební transakce.

Konečně pak sám Navrhovatel při své vlastní výpovědi popsal způsob, kdy si třetí osoba od Navrhovatele vyžádala ke Sporné platební transakci od Navrhovatele autorizační sms kód, načež jí Navrhovatel sám aktivně přeposlal celou autorizační sms zprávu.

Všechny dosud shromážděné podklady tedy svědčí závěru, že ke zneužití internetového bankovnictví Navrhovatele došlo ve sféře Navrhovatele za jeho aktivní účasti, která spočívala v přeposlání autorizační sms zprávy třetí osobě, tedy zpřístupnění personalizovaných bezpečnostních prvku třetí osobě.

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 Všeobecných podmínkách. Podpisem Smlouvy o účtu na sebe Navrhovatel převzal tyto smluvní povinnosti, jejichž účelem je i ochrana personalizovaných bezpečnostních prvků internetového bankovnictví:

a) podle článku 24.1 „Bezpečnostní údaje“ Všeobecných podmínek: *„[…] Uživatel je povinen Bezpečnostní údaje chránit před vyzrazením neoprávněné osobě, před ztrátou, odcizením a jakýmkoliv zneužitím“*.

Přiměřenost opatření, jak požaduje zákon o platebním styku, 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 považuje povinnosti uživatele platebního prostředku sjednané mezi Navrhovatelem a Institucí uvedené v bodech a) za přiměřené.

Navrhovatel by tedy za ztrátu ze Sporné platební transakce neodpovídal, pokud by ji nezpůsobil svým podvodným jednáním, nebo pokud by některou z povinností uvedených v bodech a) výše porušil úmyslně anebo z hrubé nedbalosti.

Navrhovatel a Instituce si v článku 32.3 „Odpovědnost za neautorizovanou platební transakci“ Všeobecných podmínek současně výslovně sjednali, že *„[k]lient nese ztrátu z neautorizované platební transakce v plném rozsahu, pokud tuto ztrátu způsobil svým podvodným jednáním nebo tím, že úmyslně nebo z hrubé nedbalosti porušil některou ze svých povinností dle bodu 22. a 24. VOP* (článek 22 „Bezpečnost při používání Karty“ Všeobecných podmínek se v tomto případě nepoužije, protože ke Sporné platební transakci nedošlo prostřednictvím platební karty Navrhovatele – pozn. finančního arbitra)*.“*

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

Nedbalost pak právní teorie dělí na vědomou a nevědomou. 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 č. 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 [srov. 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“*].

V tomto případě si Navrhovatel a Instituce v článku 24.4 „Ztráta, odcizení nebo zneužití Bezpečnostních údajů nebo Bezpečnostních prostředků“ Všeobecných podmínek sjednali, že *„[n]eúmyslné porušení stanovených bezpečnostních pravidel při používání služeb přímého bankovnictví, zejména pravidel pro nakládání s Bezpečnostními údaji a Bezpečnostními prostředky Klientem je hrubou nedbalostí.“*

Podle článku 3.2 „Identifikace a ověření uživatele“ Příručky služeb SERVIS 24 Instituce *„[n]ení odpovědna za prozrazení bezpečnostních prvků, pokud k prozrazení dojde na straně klienta nebo osob, které si k užívání služeb SERVIS 24 zvolí* (tj. Disponent nebo Zmocněná osoba ve smyslu článku 6 „Uživatelé ve službách SERVIS 24“ Příručky služeb SERVIS 24; ze shromážděných podkladů nevyplývá, že by si Navrhovatel zvolil Disponenta či Zmocněnou osobu a že by tyto osoby prozradily Bezpečnostní údaje třetí osobě – pozn. finančního arbitra)*.“*

Finanční arbitr ze shromážděných podkladů zjistil, že Navrhovatel porušil smluvně převzatou povinnost *„[b]ezpečnostní údaje chránit před vyzrazením neoprávněné osobě, před ztrátou, odcizením a jakýmkoliv zneužitím“* uvedenou v článku 24.1 „Bezpečnostní údaje“ Všeobecných podmínek, když přes aplikaci Messenger přeposlal uživateli označenému jako „Vojta“ autorizační sms kód a zpřístupnil tak bezpečnostní údaj třetí osobě.

Navrhovatel tvrdí, že kdyby zpráva s sms autorizačním kódem obsahovala rovněž označení čísla účtu, ze kterého se peněžní prostředky převádějí *„prověřil bych si její obsah a poté jednal.“*

Označení čísla účtu, ze kterého se peněžní prostředky odepisují, může určitě přispět k větší informovanosti klientů, nicméně žádný právní předpis neupravuje konkrétní obsah autorizačních sms zpráv. Navrhovatel však měl reagovat na zprávu i bez uvedení čísla účtu, protože se jednalo o sms zprávu Instituce.

V této souvislosti současně Navrhovatel tvrdí, že *„[…] spatřuji chybu ze strany Instituce zejména v nedostatečné informovanosti klienta (čili mne) na možná rizika při používání internetového bankovnictví Servis24. Nicméně já, jakožto běžný uživatel, jsem se s takovým upozorněním nesetkal a ani ho nikde neviděl.“*

Z otisku bezpečnostních upozornění, seznamu zpráv a bezpečnostních upozornění za období od 1. 1. 2014 do 14. 9. 2016, výstupu z informačního systému Instituce s doručením bezpečnostních upozornění a Přehledu přihlášení do internetového bankovnictví arbitr zjistil, že v rozporu s tímto tvrzení Navrhovatele Instituce Navrhovateli opakovaně zasílala bezpečnostní upozornění, kdy některá z nich si Navrhovatel i zobrazil. Dne 29. 10. 2015 v 14:21 hod. si pak Navrhovatel v internetovém bankovnictví zobrazil zprávu „Upozornění na možné zneužití internetového bankovnictví prostřednictvím Facebooku“, ve kterém Instituce detailně popisovala, jakým způsobem se útočník dostává k autorizační sms zprávě a současně upozorňovala *„Aby se podvodník dostal k potvrzovací SMS zprávě, sdělí klientovi, že má nějaký problém s telefonem, a požádá, jestli si může nechat poslat autorizační sms na telefon klienta s tím, aby mu ji klient následně přeposlal. […] Upozorňujeme, abyste na podobné zprávy v žádném případě nereagovali a nezadávali požadované údaje. […] Proto nikdy nedejte na jakkoli úpěnlivé výzvy, podoba podvodu se může časem změnit. […] Nikdy také nepřeposílejte žádné své autorizační SMS zprávy dalším osobě.“*

Sám Navrhovatel v Úředním záznamu ze dne 18. 7. 2016 tvrdí, že *„[m]ě už pak ale něco říkalo, koukni se na svůj účet, tak jsem se na něj kouknul přes telefon a zjistil jsem, že mě z účtu odešlo 140.000 Kč. […] Ještě uvádím, že nedávno asi tak před 4 až 5 měsíců mě přišlo jakoby od České spořitelny odkaz, a když jsem kliknul tak stránka servisu 24, ale protože na to Česká spořitelna poukazovala, že jde o podvod, tak jsem to nevyplňoval a smazal jsem to.“*

Z výše uvedeného tak vyplývá, že Navrhovatel věděl o existenci útoků na platební účty klientů bank v podobě podvodných e-mailů a i jemu samotnému přeposílání autorizačních sms zpráv v tomto konkrétním případě přišlo podezřelé, a přesto autorizační sms zprávy přeposílal.

Tímto jednáním Navrhovatel tak projevil jednak mimořádnou lhostejnost, lehkomyslnost a nepozornost při nakládání s bezpečnostním údajem, ale také tímto ignoroval veškeré zásady prevence negativních dopadů zneužití bezpečnostních údajů vyjádřené v článku 24.4 „Ztráta, odcizení nebo zneužití Bezpečnostních údajů nebo Bezpečnostních prostředků“ Všeobecných podmínek.

Pokud jde o konkrétní způsob, jakým se třetí osoba dostala k přihlašovacím údajům do internetového bankovnictví Navrhovatele, tedy zda k tomu došlo v důsledku virů v počítači

Navrhovatele nebo v důsledku zadání přihlašovacích údajů na podvodné webové stránce nebo do podvodné aplikace, se finančnímu arbitrovi sice nepodařilo zjistit, a to zejména i proto, že mu Navrhovatel nepředložil přehled internetové historie počítače a mobilního telefonu.

Pokud jde o přehled internetové historie mobilního telefonu Navrhovatele, finanční arbitr Navrhovatele vyzval, aby předložil přehled internetové historie mobilního telefonu Navrhovatele za období jednoho měsíce před provedením Sporné platební transakce, načež Navrhovatel nejdříve předložil finančnímu arbitrovi historii za období od 20. 6. 2016 do 5. 7. 2016. Poté Navrhovatel finančnímu arbitrovi sdělil, že historii z mobilního telefonu musí provést specializovaná firma, protože sám to neumí. Následně Navrhovatel předložil finančnímu arbitrovi Servisní protokol, ze kterého vyplývá, že z telefonního přístroje značky „Cubot X 11“, „seriové číslo [redacted]“ nelze vyjmou data z historie prohlížeče za období od 17. 6. 2016 do 17. 7. 2016.

Z výše uvedeného není finančnímu arbitrovi zřejmé, proč Navrhovatel byl schopen předložit přehled historie mobilního telefonu za období od 20. 6. 2016 do 5. 7. 2016, ale pro další období bylo potřeba specializovaného servisu. Současně finanční arbitr zjistil, že mobilní telefon, který Navrhovatel odnesl do servisu a na základě kterého předložil Servisní protokol, je přístrojem jiné značky, než který Navrhovatel používal v době Sporné platební transakce, když z Úředních záznamů z 18. 7. 2016 a z 19. 7. 2016 vyplývá, že používal přístroj značky *„Xaoimi redminton 3“ pro ([redacted]), od kamaráda […]”, „Dále také poskytuji policii svůj mobilní telefon XIAOMI RED MI NOTE 3 PRO, pro provedení kopie jeho obsahu, resp. provedení bitové kopie pro jeho zkoumání“.*

Pokud jde o přehled internetové historie počítače, Navrhovatel předložil finančnímu arbitrovi dva soubory, z nichž jeden označil za historii prohlížeče za měsíc červen a druhý za měsíc červenec 2016. Finanční arbitr zjistil, že oba soubory byly totožné, ale pouze ve formátu prostého textu a navíc z nich nebyly patrné data a časy navštívení jednotlivých webových stránek. Proto finanční arbitr vyzval Navrhovatele k předložení přehledu internetové historie počítače opakovaně. Navrhovatel finančnímu arbitrovi sdělil, že historii z počítače musí provést specializovaná firma, protože sám to neumí. Poté Navrhovatel finančnímu arbitrovi sdělil, že servis nemohl dohledat historii prohlížeče v počítači, protože se řídil pokyny pracovnice Instituce a systém nechal přeinstalovat.

Z výše uvedeného tak není zřejmé, z jakého zdroje a kdy Navrhovatel pořídil soubory, které předložil finančnímu arbitrovi, a kdy provedl přeinstalaci počítače.

Současně Navrhovatel v odstranění nedostatků návrhu tvrdí, že *„[…] novou instalaci operačního systému jsem na žádost PČR zatím neprováděl, mobilní telefon jsem také, na žádost PČR, do továrního nastavení neuvedl […].”*

V Úředním záznamu z 25. 8. 2016 Navrhovatel tvrdí, že *„[…] pro finančního arbitra mám zajištěnou historii prohlížeče jak mobilního telefonu, tak i počítače a to v době jednoho měsíce před samotným útokem, kdy toto doložím do 5. 9. 2016, […].“*

Navrhovatel rovněž nedoložil ani své tvrzení, že *„[a]ntivirový program byl stále zapnutý a aktualizovaný.“*

Navrhovatel finančnímu arbitrovi nikdy pro řízení relevantní přehled historie mobilního telefonu a počítače před Spornou platební transakci nepředložil.

Přesto však lze ze všech podkladů, které finanční arbitr shromáždil dovodit, že k vyzrazení přístupových údajů do internetového bankovnictví muselo dojít ve sféře Navrhovatele, který nadto neobyčejně lehkovážně přistoupil k přeposílání autorizačních sms zpráv, ačkoli jej Instituce v období od 1. 1. 2014 do 14. 9. 2016 opakovaně upozorňovala na nebezpečí

spojená s podvody prostřednictvím facebooku a žádostmi tzv. kamarádů o přeposílání sms zpráv.

Finanční arbitr se tak hlásí k závěrům, které ve svých rozhodnutích vyslovil Nejvyšší soud. Podle Nejvyššího soudu *„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“* (usnesení Nejvyššího soudu ze dne 4. 6. 2008, sp. zn. 28 Cdo 1938/2008). Obdobně dále Nejvyšší soud ve svém rozhodnutí sp. zn. 21 Cdo 2682/2013 ze dne 26. 6. 2014 dochází 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) …“.*

Přestože finanční arbitr tedy nezjistil konkrétní způsob, jakým došlo ve sféře Navrhovatele k zneužití jeho přihlašovacích údajů do internetového bankovnictví, lze ze shromážděných podkladů dovodit, že kdyby Navrhovatel nepřeposlal autorizační sms zprávy prostřednictvím aplikace Messenger, nikdy by v jeho případě k neautorizovaným platebním transakcím nedošlo.

Finanční arbitr nezjistil, že by Navrhovatel způsobil ztrátu ze Sporné platební transakce podvodně nebo úmyslně, ale tím, že z hrubé nedbalosti porušil zákonnou a smluvně převzatou povinnost, a to povinnost chránit bezpečnostní údaj před vyzrazením neoprávněné osobě, před ztrátou, odcizením a jakýmkoliv zneužitím vyplývající z § 101 zákona o platebním styku ve spojení s článkem 24.1 „Bezpečnostní údaje“ Všeobecných podmínek.

9 <u>K výroku nálezu</u>

Protože Instituce v části návrhu Navrhovateli vyhověla a Navrhovatel vzal v této části svůj návrh na zahájení zpět, finanční arbitr výrokem I. v této části řízení zastavil.

Odpovědnost za ztrátu ze Sporné platební transakce nese Navrhovatel podle § 116 odst. 1 písm. b) ve spojení s § 101 odst. a) a b) zákona o platebním styku v plném rozsahu, a proto finanční arbitr výrokem II. v této části návrh zamítl.

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

Poučení:

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.

Mgr. Monika Nedelková
finanční arbitr

Doručuje se
Navrhovatel – do vlastních rukou na adresu [redacted]
Instituce – datová schránka wx6dkif