Obchodné podmienky
pre elektronickú správu účtov

vedených bankou **Fio banka, a.s.**, IČ: 61858374, V Celnici 1028/10, 117 21 Praha 1, Česká republika, zapísanou v obchodnom registri vedenom Mestským súdom v Prahe, oddiel B, vložka 2704, prostredníctvom organizačnej zložky **Fio banka, a.s., pobočka zahraničnej banky**, IČO: 36869376, Nám. SNP 21, 811 01 Bratislava, zapísanej v obchodnom registri vedenom Okresným súdom Bratislava I, oddiel: Po, vložka č.: 1875/B (ďalej aj len „Banka“)

Čl. I. Predmet úpravy

1. Banka umožňuje svojim klientom na základe zmluvy o elektronickej správe účtov (ďalej len „zmluva“) elektronicky spravovať ich účty vedené Bankou, prípadne priamo bankou Fio banka, a.s., IČ: 61858374, ČR (ďalej tiež len „internetbanking“). Ak sa ďalej píše o internetbankingu, môže tým byť podľa povahy úpravy myslený taktiež tzv. „smartbanking“, teda služba priameho bankovníctva, pomocou ktorej Banka umožňuje svojim klientom na základe zmluvy elektronicky spravovať ich účty vedené Bankou, a to použitím na tento účel Bankou určenej aplikácie smartbanking v klientovom mobilnom zariadení. Pre smartbanking platia všetky nasledujúce ustanovenia rovnako ako pre internetbanking, ak nie je ďalej uvedené inak. Elektronickou správou účtov sa rozumie bezdokladové elektronické podávanie pokynov a využívanie ďalších služieb poskytovaných k účtu a získavanie informácií o účte a vykonaných službách. Oprávnenie na elektronickú správu účtu fyzickej osoby môže udeliť majiteľ účtu elektronicky v prospech tretej fyzickej osoby - klienta Banky určením jeho prihlasovacieho mena a prideleného identifikačného čísla klienta. Oprávnenie na elektronickú správu účtu právnickej osoby môže udeliť písomne v prospech tretej fyzickej osoby osoba oprávnená konať za právnickú osobu. Súčasne určí majiteľ účtu aj rozsah splnomocnenia, tzn. určí, ktoré úkony je splnomocnená osoba oprávnená vykonávať. Splnomocnená osoba spravuje účet majiteľa v medziach splnomocnenia svojím vlastným prihlasovacím menom, heslom a zvoleným spôsobom autorizácie elektronickej komunikácie.
2. Tieto obchodné podmienky pre elektronickú správu účtov (ďalej tiež len Podmienky) doplňujú alebo podrobnejšie upravujú niektoré ustanovenia zmluvy, prípadne k nim uvádzajú záväzný výklad. V prípade rozporu medzi úpravou v zmluve a Podmienkach platia ustanovenia zmluvy.

Čl. II. Spôsob prenosu a zabezpečenia prenášaných dát

1. Všetky pokyny a informácie, ktoré sa dajú podať, resp. získať pomocou elektronickej správy účtov, sú prenášané medzi serverom Fio banky, a.s. a počítačom či obdobným mobilným zariadením, ako napríklad tzv. chytrým telefónom (smartphone) či tabletom, (ďalej aj len súhrnné označenie „zariadenie“ pre počítač, mobilný telefón, tablet a obdobné mobilné zariadenia) klienta prostredníctvom internetu. Adresa serveru Banky je: www.fio.sk; ďalšie adresy Banky sú: www.fio.cz, www1.fio.cz, www2.fio.cz, www3.fio.cz, www.fiobanka.com, www.fio.hu, www.e-broker.cz, ib.fio.cz, ib.fio.sk. Banka má právo kedykoľvek obmedziť prístup na ktorýkoľvek zo serverov Banky, a to dočasne aj natrvalo. Prenášané dáta sú zabezpečené prostredníctvom šifrovanej komunikácie (https) za pomoci certifikátu SSL serveru od spoločnosti GeoTrust Inc.

2. Klient je pred každým využitím služieb Banky poskytovaných prostredníctvom internetu (predovšetkým služieb Internetbanking a e-Broker) a pred každým zadaním dôverných údajov do prihlasovacieho dialógu povinný najskôr overiť, či sú z jeho strany dodržané všetky povinnosti uložené v ods. 1 čl. XIII. „Bezpečnostné opatrenia vo sfére vplyvu klienta, zabezpečenie zariadení klienta“. Banka nezodpovedá za škodu spôsobenú porušením tejto

povinnosti. Ďalšie povinnosti klienta súvisiace s obmedzením rizík pri používaní služieb Banky prostredníctvom internetu, ako aj dôležité informácie a upozornenia na riziká, ktoré sa týkajú využívania služieb Banky prostredníctvom internetu, sú uvedené v čl. IX. až XVa Podmienok.

3. Banka zriaďuje klientovi prístup na neverejné stránky servera Banky pomocou užívateľského mena a hesla, ktoré si klient zvolí a dohodnutým spôsobom odovzdá Banke. Klient je oprávnený heslo kedykoľvek zmeniť.

Čl. III. Autorizácia elektronicky zadaných pokynov

1. Elektronicky podané pokyny musia byť klientom autorizované, tzn. podpísané jedným z nižšie uvedených spôsobov alebo ich kombináciou, v závislosti od spôsobu zvoleného klientom, prípadne stanoveného Bankou v čl. VII Podmienok. Pokyny podané elektronicky pomocou smartbankingu musia byť klientom autorizované zadaním PINu pre smartbanking, pričom tento spôsob autorizácie nie je možné kombinovať s ostatnými spôsobmi. Aplikácia smartbanking môže na niektorých mobilných zariadeniach umožniť nahradenie PINu pre smarbanking alebo prístupových údajov pre smartbanking (vždy však maximálne jedného z týchto bezpečnostných prvkov) použitím zabudovaného biometrického snímača. Ak bol pokyn autorizovaný, má sa za to, že klient súhlasil s podaním a vykonaním pokynu, ak klientom nie je preukázané, že pokyn neautorizoval.
2. **Autorizácia elektronickým podpisom**. Banka dodá klientovi program, ktorý mu umožní vytvoriť si vlastný elektronický podpis – šifrovací kľúč. Klient je oprávnený po začatí elektronickej komunikácie zmeniť šifrovací kľúč. Zmenu šifrovacieho kľúča uskutoční klient tak, že v programe dodanom Bankou si vytvorí nový šifrovací kľúč, ktorého verejnú časť zašle Banke pokynom prostredníctvom internetbankingu alebo jej ho osobne poskytne na jej pracovisku. V prípadoch, kedy Banka prostredníctvom internetbankingu vyzve klienta k zmene šifrovacieho kľúča, je klient povinný túto zmenu uskutočniť v lehote uvedenej vo výzve. V opačnom prípade Banka šifrovací kľúč po márnom uplynutí lehoty zruší. Po zrušení šifrovacieho kľúča nebude klient môcť uskutočňovať pokyny, ktoré vyžadujú autorizáciu podľa čl. VII ods. 9 Podmienok, a to do doby, dokiaľ neuskutoční zmenu šifrovacieho kľúča zhora uvedeným spôsobom. Verejnú časť svojho šifrovacieho kľúča odovzdá klient osobne Banke pred spustením elektronickej komunikácie. Správa prístupu k tajnej časti šifrovacieho kľúča a k heslu kľúča je plne v zodpovednosti klienta. Ak je klientom právnická osoba, musí každá fyzická osoba, ktorá je oprávnená v mene klienta podávať pokyny a získavať informácie, mať svoje užívateľské meno a heslo, ktoré je považované za užívateľské meno a heslo klienta, a svoj šifrovací kľúč, ak si zvolila autorizáciu elektronickým podpisom. Manuál pre elektronickú aplikáciu Fio-podpis, určený pre inštaláciu a použitie elektronického podpisu, je možné získať na každej pobočke Banky alebo na webovej stránke Banky: http://www.fio.sk/spolocnost-fio/manualy-dokumenty-cenniky/manualy. Klient je povinný pri inštalácii a použití elektronického Fio-podpisu postupovať podľa uvedeného manuálu. Autorizáciu pokynu prostredníctvom elektronického Fio-podpisu vykonáva klient uvedením svojho hesla k súkromnej časti elektronického Fio-podpisu (šifrovacieho kľúča) do príslušného poľa formulára pre zadávanie pokynov v rámci internetbankingu po tom, čo sa riadne prihlásil do internetbankingu svojím prihlasovacím menom a prístupovým heslom. Následne je vygenerovaná verejná časť elektronického Fio-podpisu, ktorá je zaslaná Banke. Banka overí zhodu zaslanej verejnej časti elektronického Fio-podpisu s verejnou časťou elektronického Fio-podpisu, ktorá bola uložená u Banky. Ak je zaslaná a uložená verejná časť elektronického Fio-podpisu zhodná, je pokyn autorizovaný.
3. **Autorizácia jednorazovým sms kódom**. Klient oznámi Banke telefonické číslo, na ktoré bude Banka klientovi zasielať sms správy s jednorazovým autorizačným kódom. Autorizačný kód je určený vždy k jednoznačne definovanému pokynu. Klient si v rámci nastavenia podmienok autorizácie môže spomedzi možností ponúkaných Bankou zvoliť dĺžku autorizačného kódu (5 – 25 znakov), počet pokusov pre zadanie kódu (1 – 5 pokusov) a platnosť autorizačného kódu (max. 20 minút). V prípade prepadnutia platnosti autorizačného kódu (vygenerovania nového autorizačného kódu k zadanému pokynu, uplynutiu stanovenej doby platnosti) klient môže požiadať o zaslanie nového jednorazového

autorizačného kódu. Autorizáciu pokynu prostredníctvom sms kódu vykonáva klient uvedením zaslaného sms kódu do príslušného poľa formulára pre zadávanie pokynov v rámci internetbankingu po tom, čo sa riadne prihlásil do internetbankingu svojím prihlasovacím menom a prístupovým heslom. Ak je klientom vložený sms kód zhodný s sms kódom vygenerovaným a zaslaným Bankou, je pokyn autorizovaný.

3a. **Autorizácia PINom pre smartbanking.** Pre používanie smartbankingu si klient do svojho mobilného zariadenia opatrí Bankou určenú aplikáciu smartbanking umožňujúcu poskytovanie tejto služby podľa operačného systému mobilného zariadenia (na internetových stránkach Banky je možné nájsť odkazy na autorizované zdroje tejto aplikácie). Bankou určenými aplikáciami smartbanking nemusia byť podporované všetky typy mobilných zariadení a ich operačné systémy. Klient zriadi používanie smartbankingu pokynom v internetovom rozhraní internetbankingu spoločne so zadaním prístupového hesla smartbankingu a zadaním unikátneho identifikačného kódu (ďalej len „UID“) mobilného zariadenia, ktoré bude pre prístup k smartbankingu používané (pričom z iného mobilného zariadenia nebude prístup umožnený). Tento pokyn musí byť riadne autorizovaný elektronickým podpisom a/alebo jednorazovým sms kódom, v závislosti od spôsobu autorizácie zvolenej klientom. Ak bude chcieť klient prostredníctvom smartbankingu podávať pokyny, je nevyhnutné zriadiť v internetovom rozhraní internetbankingu PIN pre smartbanking a tento PIN riadne autorizovať elektronickým podpisom a/alebo jednorazovým sms kódom, v závislosti od spôsobu autorizácie zvolenej klientom. Autorizáciu pokynu prostredníctvom PINu pre smartbanking vykonáva klient zadaním PINu pre smartbanking do príslušného pola pre zadávanie pokynov v aplikácii smartbanking po tom, čo sa riadne prihlásil do smartbankingu svojím prihlasovacím menom a heslom smartbankingu.

3b. **Autorizácia za použitia biometrického snímača.** Pokiaľ je už nastavený spôsob autorizácie podľa ods. 3a, na vybraných mobilných zariadeniach môže aplikácia smartbanking umožniť nahradenie PINu pre smartbanking alebo prístupových údajov pre smartbanking (vždy však maximálne jedného z týchto bezpečnostných prvkov) použitím zabudovaného biometrického snímača. Možnosť použitia biometrického snímača klient nastaví v aplikácii smartbanking a jeho nastavenie autorizuje PINom pre smartbanking. Pred nastavením použitia biometrického snímača banka odporúča klientovi zoznámiť sa s princípmi jeho fungovania v použitom mobilnom zariadení. Banka nezodpovedá za správne fungovanie biometrického snímača a klient nastavením jeho použitia pre smartbanking na seba preberá riziko vyplývajúce z možných chýb spojených s jeho fungovaním. Aplikácia smartbanking ani iné systémy banky nezískavajú, nespracovávajú ani neukladajú žiadne biometrické dáta klienta. Zrušenie možnosti použitia biometrického snímača sa nastavuje potvrdením príslušnej voľby v smartbankingu.

Pre alternatívnu autorizáciu pomocou passcode do telefónu platia rovnaké pravidlá a povinnosti ako pre autorizáciu pomocou biometrického snímača.

4. Nastavenie spôsobu a podmienok autorizácie podľa ods. 2 a 3 konkrétneho klienta je uvedené v Zmluve, prípadne v Protokole o nastavení autorizácie elektronických pokynov. Nastavenie spôsobu a podmienok autorizácie PINom pre smartbanking podľa ods. 3a a prípadné následné nastavenie autorizácie použitím biometrického snímača podľa ods. 3b je považované za nastavenú autorizáciu elektronických pokynov podľa Zmluvy o elektronickej správe účtov okamžikom zriadenia smartbankingu klientom prostredníctvom internetového rozhrania internetbankingu (resp. okamihom nastavenia použitia biometrického snímača podľa ods. 3b), i keď tento spôsob autorizácie nie je uvedený v Zmluve či v Protokole o nastavení autorizácie elektronických pokynov.

5. Spôsob a podmienky autorizácie podľa ods. 2 a 3 môže klient meniť osobne na pobočke Banky. Spôsob a podmienky autorizácie podľa ods. 3a môže klient meniť elektronicky prostredníctvom internetového rozhrania internetbankingu. Spôsob a podmienky autorizácie podľa ods. 3b môže klient zmeniť elektronicky prostredníctvom aplikácie smartbanking.

Čl. IV. Zriaďovanie a rušenie podúčtov bežného účtu a rušenie účtov pomocou elektronickej správy

1. Prostredníctvom elektronickej správy účtov sa dajú zriaďovať a rušiť podúčty bežného účtu (ďalej len podúčty), ak to je výslovne uvedené ako jedna z možností v čl. VII. podmienkou pre zriaďovanie podúčtov je uzatvorenie a platnosť príslušného dodatku k zmluve o vedení bežného účtu.
2. Prostredníctvom elektronickej správy účtov sa dajú tiež rušiť účty, s výnimkou bežných účtov, Fiokonta, bežných vkladov, špeciálnych bežných účtov a účtov, o ktorých to stanoví Zmluva o vedení účtu alebo Obchodné podmienky pre zriaďovanie a vedenie účtov (vydávané Bankou, príp. vydávané priamo bankou Fio banka, a.s., ak ide o elektronickú správu účtu vedeného priamo bankou Fio banka, a.s.), aj keď neboli založené pomocou elektronickej správy účtov, pokiaľ sa Banka a klient nedohodnú inak. Po dobu jedného roka odo dňa zrušenia účtu môže klient naďalej získavať všetky informácie o účte či podúčte, vrátane pohybov na účte či podúčte.

Čl. V. Rozsah zodpovednosti strán

1. Klient zodpovedá za záväzky vzniknuté elektronickým podaním pokynu rovnako, ako by bol pokyn alebo žiadosť podaná písomne.
2. Klient zodpovedá za logickú správnosť a súlad všetkých svojich elektronicky podaných pokynov so zmluvou a Podmienkami, prípadne ďalšími predpismi.
3. Klient zodpovedá za škodu, ak škodu spôsobil svojím podvodným konaním, úmyselným nesplnením povinnosti používať internetbanking podľa podmienok uvedených v zmluve či Podmienkach, úmyselným nesplnením povinnosti podľa čl. XVa alebo úmyselným porušením povinnosti vykonať všetky primerané úkony na zabezpečenia dôverných údajov, alebo z hrubej nedbanlivosti. Hrubou nedbanlivosťou sa rozume porušenie akejkoľvek povinnosti klienta vyplývajúcej z článku II, III,VIII, IX, XI až XIV, XV a XVa týchto podmienok, najmä porušenie opatrení za účelom zaistenia bezpečnosti a utajenia dôverných údajov, porušenie povinností na zabezpečenie zariadenia používaného pre prístup do internetbankingu, porušenie povinností na zabezpečenie mobilného zariadenia/SIM karty používanej na zasielanie SMS kódov, porušenie povinnosti overiť identifikáciu servera Banky alebo aplikácie pre elektronický podpis alebo porušenie povinnosti včas oznámiť Banke podozrenie na zneužitie bezpečnostných údajov.
4. Klient neznáša nijaké finančné dôsledky vyplývajúce zo zneužitia internetbankingu od okamihu oznámenia skutočnosti podľa článku XVa okrem prípadov, keď konal podvodným spôsobom.
5. Klient znáša stratu až do 100 eur, ktorá súvisí so všetkými neautorizovanými platobnými operáciami vykonanými prostredníctvom internetbankingu a ktorá je spôsobená zneužitím internetbankingu neoprávnenou osobou v dôsledku nedbanlivosti klienta pri zabezpečovaní dôverných údajov, t.j. v dôsledku nedbanlivosti pri plnení povinnosti klienta vykonať všetky primerané úkony na zabezpečenia dôverných údajov (ako personalizovaných bezpečnostných prvkov internetbankingu), ak v zmluve či Podmienkach nie je uvedené inak. Primeranými úkonmi na zabezpečenie ochrany dôverných údajov sa na účely tohto článku považujú všetky úkony na zabezpečenie ochrany dôverných údajov, ktoré sú uvedené v zmluve a Podmienkach.
6. Banka zodpovedá za bezchybnosť spracovania požiadaviek klienta, ktoré sú jej odovzdané v súlade so zmluvou a Podmienkami. Banka nenesie žiadnu zodpovednosť za prípadné škody vzniknuté z dôvodu poruchy prenosovej siete alebo z dôvodu náhody, t.j. nepredvídateľnej a na vôli Banky nezávislej udalosti, ktorej následky nemohla Banka odvrátiť.
7. Banka zodpovedá za nesprávne vykonanie pokynu, ibaže klientovi doloží, že čiastka nesprávne vykonaného pokynu bola riadne a včas pripísaná na účet poskytovateľa platobných služieb príjemcu.

8. Banka nezodpovedá za platobnú operáciu vykonanú na základe neautorizovaného pokynu alebo za chybne vykonanú platobnú operáciu, ak klient neoznámil túto skutočnosť Banke bez zbytočného odkladu odo dňa zistenia neautorizovanej alebo chybne vykonanej platobnej operácie, najneskôr však do 13 mesiacov odo dňa odpísania peňažných prostriedkov, z príslušného účtu.¨

Čl. VI. Zmluvná odmena a poplatky

1. Výška odmeny účtovaná Bankou za umožnenie elektronické správy účtov je uvedená v Cenníku finančných operácií a služieb, ktorý vydáva Banka. Cenník môže byť vydaný vo forme niekoľkých čiastkových cenníkov. Náklady na komunikáciu s Bankou hradí klient.
2. Poplatky za vykonané pokyny zadané pomocou elektronickej správy účtov a poplatky za využitie informačných a autorizačných prostriedkov sú rovnako uvedené v Cenníku finančných operácií a služieb.

Čl. VII. Pokyny a informácie, ktoré sa dajú podávať, resp. získavať prostredníctvom el. správy účtov

1. Prostredníctvom internetbankingu, ktorý slúži ako komunikačný program medzi Bankou a klientom, je klient hlavne oprávnený zadávať pokyny Banke, prijímať od Banky informácie, správy, upozornenia, ponuky na platobné a bankové služby, uzatvárať s Bankou konkrétne zmluvy a tiež inak komunikovať s Bankou. Z toho dôvodu je klient povinný sledovať všetky správy, informácie a upozornenia, ktoré mu Banka prostredníctvom internetbankingu doručí. Neplnenie tejto povinnosti je porušenie povinností vyplývajúcich zo zmluvy.
2. Klient súhlasí s tým, že Banka v prípadoch, kde to právne predpisy nevylučujú, bude používať naskenovaný podpis ako mechanický prostriedok náhrady vlastnoručného podpisu v zmluvných vzťahoch s klientom založených Zmluvou a upravených týmito Podmienkami. Klient berie na vedomie, že takúto prax považuje Banka za obvyklú.
3. Banka i klient súhlasia, že v rámci kontaktu klienta s Bankou prostredníctvom internetbankingu bude autorizácia pokynov klienta v internetbankingu považovaná za mechanický prostriedok náhrady jeho vlastnoručného podpisu, kde to právne predpisy nevylučujú. Klient prehlasuje, že takúto prax berie za obvyklú.
4. Klient súhlasí, že Banka má právo používať internetbanking, e-mailové správy, kuriéra, službu krátkych textových správ (SMS) alebo iný prostriedok diaľkovej komunikácie umožňujúci komunikáciu s klientom s cieľom ponúknuť mu akékoľvek služby spojené so zriadením bežného účtu. Klient súhlasí s poskytnutím akýchkoľvek informácií, materiálov a ponúk spôsobom uvedeným v predchádzajúcej vete tohto odseku.
5. V prípadoch, kedy Banka bude klientovi doručovať akýkoľvek dokument prostredníctvom internetbankingu, bude sa dokument považovať za doručený v momente, keď Banka dostane potvrdenie o jeho prečítaní zo strany klienta, najneskôr však dňom nasledujúcom po odoslaní dokumentu, pokiaľ klient nepreukáže, že sa z dôvodov nezávislých na jeho vôli nemohol s obsahom zaslaného dokumentu zoznámiť.
6. V prípadoch doručovania kuriérom sa považuje za deň doručenia deň prijatia zásielky klientom.
7. Ak je príslušná služba Bankou poskytovaná a ak nie je ďalej uvedené inak, v internetbankingu sa dajú podávať tieto pokyny:

a) podanie/zmena/rušenie riadnej výpovede na vklad s výpovednou lehotou alebo na sporiaci účet s výpovednou lehotou,
b) prevodný príkaz (príkaz na prevod finančných prostriedkov),
c) odvolanie prevodného príkazu, ktorého splatnosť ešte len nastane,
d) trvalý prevodný príkaz z bežného účtu alebo bežného vkladu,
e) zmena/rušenie trvalého prevodného príkazu z bežného účtu alebo bežného vkladu,
f) zriadenie/zmena/zrušenie súhlasu s inkasom v prospech iného účtu,
g) zriadenie/zmena/zrušenie súhlasu s platbami SIPO,
h) avizovanie výberu hotovosti pobočke Banky,

i) zriaďovanie podúčtov a rušenie podúčtov, rušenie účtov[1] s výnimkou účtov podľa čl. IV. ods. 2 Podmienok,
j) zmena spôsobu pripisovania úrokov, dispozícia s úrokmi a dispozícia so zostatkom účtu alebo podúčtu po jeho zrušení,
k) zmena hesla (pre internetbanking či smartbanking),
l) splnomocnenie tretej osoby na správu účtu majiteľa,
m) zriadenie/zrušenie informačného hlásiča o udalostiach na účte,
n) zriadenie/zrušenie smartbankingu a zadanie prístupového hesla pre smartbanking a UID mobilného zariadenia pre smartbanking,
o) zriadenie/zmena/zrušenie PINu pre smartbanking,
p) zmena UID mobilného zariadenia pre smartbanking,
q) zmena spôsobu a frekvencie zasielania výpisov z účtov,
r) prijímať predschválené ponuky Banky na poskytnutie ďalších služieb v rámci zriadenia bežného účtu či podúčtu,
s) zaslať Banke návrh na uzatvorenie zmluvy o poskytovaní bankových či platobných služieb,
t) zmena šifrovacieho kľúča,
u) uzatvorenie zmluvy o vydaní platobnej karty,
v) voľba/zmena vlastného PINu,
w) zmena výšky limitu pre platobné karty,
x) stavu platobnej karty,
y) voľba použitia biometrického snímača v mobilnom zariadení pre smartbanking (toto možno nastaviť iba cez smartbanking)

8. Elektronickou správou účtov sa dajú získavať najmä tieto informácie:
a) parametre účtov a podúčtov,
b) zostatok na účte alebo podúčte k určitému dátumu,
c) pohyby na účte alebo podúčte za určité obdobie (správy o zúčtovaní položiek),
d) výpis z účtu alebo podúčtu,
e) parametre vydanej platobnej karty,
f) prehľad podaných pokynov spolu s ich stavmi, a pod.

9. Niektoré z pokynov podľa ods. 7, podľa požiadaviek Banky týkajúcich sa autorizácie a aktuálnych v čase zadávania pokynu, musia byť autorizované podľa čl. III. Podmienok. Niektoré z pokynov a informácií, ktoré možno podávať resp. získavať prostredníctvom el. správy účtov, uvádzané v ods. 7 a 8, môžu byť pri použití smartbankingu obmedzené v závislosti od verzie aplikácie, mobilného zariadenia či jeho operačného systému.

10. Elektronickou správou účtov je možné zadať požiadavku na založenie alebo zrušenie informačného hlásiča o niektorých udalostiach na účte. Klient si môže zvoliť hlásič podľa aktuálnej ponuky prístupnej klientovi v rámci elektronickej správy účtov. Klient je oprávnený zvoliť možnosť zasielania informácií o udalostiach na účte formou sms alebo e-mailu na ním zadaný kontakt.

11. Príkazom k úhrade sa pre účely Podmienok rozumie aj príkaz k tzv. dobitiu kreditu (ak podanie takého príkazu Banka umožňuje; Banka môže takýto príkaz označiť aj iným obdobným názvom zrozumiteľným pre bežného klienta), tj. príkaz k úhrade finančných prostriedkov v prospech účtu príslušného mobilného operátora za účelom dobitia kreditu SIM karty (tj. za účelom predplatenia služieb poskytovaných mobilným operátorom jeho zákazníkovi) identifikovanej klientom pri zadávaní pokynu uvedením telefónneho čísla príslušnej SIM karty; klient pri zadaní pokynu nezadáva číslo účtu mobilného operátora (príjemcu prevodu), ale zadá telefónne číslo príslušnej SIM karty, ktorej kredit má byť prevodom dobitý, prípadne určí aj príslušného mobilného operátora (ak je to vyžadované) a zadá iné Bankou požadované údaje.

Čl. VIII. Bezpečnostné upozornenia súvisiace s využívaním internetbankingu

[1] Rušiť účty, prípadne inak nakladať s účtami, môže iba majiteľ účtu a osoba na to majiteľom účtu splnomocnená.

1. V súvislosti s využívaním elektronických komunikačných služieb si Banka dovoľuje informovať klienta o niektorých bezpečnostných rizikách s tým spojených a zároveň si dovoľuje upozorniť klienta na základné možnosti, ktorými môže ako užívateľ ochrániť svoje osobné údaje, prihlasovacie meno a prístupové heslo do internetbankingu, elektronický kľúč, heslo chrániace elektronický kľúč, PIN pre smartbanking, prípadne zaslaný sms kód, telefónne číslo, UID mobilného zariadenia, kód (passcode, PIN) pre prístup k mobilnému zariadeniu a iné dôverné alebo citlivé údaje (ďalej tiež „dôverné údaje“) a zariadenie pred ich zneužitím. Ide o základné pravidlá, ktoré je potrebné dodržiavať na ochranu dôverných údajov a zariadenia klienta.
2. Banka a klient berú na vedomie, že zaistenie bezpečnosti dôverných informácií pri využívaní elektronických komunikačných služieb je zodpovednosťou obidvoch zmluvných strán v rozsahu ich sféry vplyvu, a že zavedenie a dodržiavanie niektorých preventívnych opatrení môže vyžadovať finančné náklady.
3. Banka je povinná na svoje náklady vykonať vo svojej sfére vplyvu také technické a organizačné opatrenia za účelom zaistenia bezpečnosti dôverných údajov, ktoré sú s ohľadom na obvyklé riziká porušenia ochrany dôverných údajov technicky možné a primerané.
4. Klient je povinný na svoje náklady vykonať vo svojej sfére vplyvu také technické opatrenia za účelom zaistenia bezpečnosti dôverných údajov, ktoré sú s ohľadom na obvyklé riziká porušenia ochrany dôverných údajov technicky možné a primerané. Klient berie na vedomie riziká spojené s využívaním elektronických komunikačných služieb a zaväzuje sa dodržiavať hlavne nižšie uvedené preventívne a bezpečnostné opatrenia a postupy na zabezpečenie bezpečnosti dôverných údajov. Nedodržanie týchto pravidiel a opatrení môže viesť k zneužitiu dôverných údajov a k vzniku škody klientovi alebo tretej osobe.
5. S ohľadom na čo najvyššiu ochranu dôverných údajov a majetku klienta odporúča Banka, aby si klient dohodol s Bankou autorizáciu elektronických pokynov pomocou sms správ alebo autorizáciu prostredníctvom elektronického podpisu a aby využíval pre zadávanie svojho hesla pri prihlasovaní do internetbankingu grafickú klávesnicu.

Čl. IX. Riziká plynúce z využívania elektronických komunikačných služieb

1. Elektronické komunikačné služby sú poskytované prostredníctvom dátových prípadne telefónnych liniek (ďalej tiež „dátové linky“), ktoré neprevádzkuje Banka, ale tretia osoba odlišná od Banky. Zabezpečenie týchto dátových liniek je mimo sféry vplyvu Banky a Banka preto nie je schopná úplne zabrániť všetkým možným rizikám zneužitia dôverných údajov v priebehu prenosu prostredníctvom dátovej linky. Pri prenose dôverných údajov nemožno preto úplne vylúčiť riziko neoprávneného získania dôverných informácií treťou osobou (napr. hrozba tzv. hackerov, interné riziká prevádzkovateľa dátovej siete, tzv. Man in the middle, t.j. odpočúvanie komunikácie treťou osobou predstierajúcou protistranu komunikácie, odpočúvanie telefonických hovorov, podvrhnutie dát a pod.).
2. Niektoré riziká plynúce z využívania elektronických komunikačných služieb môžu byť tiež vo sfére vplyvu klienta. Medzi tieto riziká patrí predovšetkým nedostatočné zabezpečenie zariadenia klienta, ktorý je používaný pre prihlásenie do internetbankingu a na podávanie pokynov Banke a ďalej nesprávne nakladanie s dôvernými údajmi klientom a z toho plynúca možnosť ich zneužitia zo strany tretích osôb.
3. Banka nezodpovedá za prípadnú škodu klienta alebo tretích osôb vzniknutú zneužitím dôverných informácií neoprávnene získaných z dátových liniek mimo sféru vplyvu Banky, zariadenia klienta alebo v dôsledku nesprávneho nakladania s týmito údajmi klientom, pokiaľ nejde o prípad porušenia povinností na strane Banky.

Čl. X. Preventívne opatrenia vykonávané Bankou

1. Banka vykonáva vo svojej sfére vplyvu preventívne opatrenia znižujúce riziko zneužitia dôverných informácií.

Medzi tieto opatrenia patrí hlavne šifrovanie všetkých dát (t.j. napr. užívateľské meno a heslo do internetbankingu), ktoré sú prenášané medzi zariadením klienta a

serverom Banky. Všetky dáta sú šifrované štandardom SSL 128bit. Šifrovanie prenášaných dát výrazne znižuje možnosť zistenia dôverných údajov o klientovi treťou osobou pri prenose dátovou linkou a ich následného zneužitia.

2. Banka ďalej umožňuje klientovi využívať ďalšie bezpečnostné prvky chrániace prístup do internetbankingu, medzi ktoré patrí možnosť využitia grafickej klávesnice pre zadávanie hesla pri prihlasovaní do internetbankingu, čo znižuje riziko neoprávneného zistenia týchto údajov treťou osobou a možnosť potvrdzovania elektronických pokynov klienta, podľa Protokolu o nastavení autorizácie elektronických pokynov, formou sms správ na individuálne stanovené telefónne číslo klienta alebo formou elektronického podpisu.
3. Informácie o niektorých bezpečnostných opatreniach súvisiacich s využívaním internetbankingu sú uvedené tiež na tejto webovej adrese: http://www.fio.sk/bankove-sluzby/internetbanking.

Čl. XI. Utajenie dôverných údajov

1. Klient je povinný chrániť svoje dôverné údaje pred zverejnením a zneužitím.
2. Klient je povinný nezaznamenávať si dôverné údaje. Ak si však klient dôverné údaje napriek tomu zaznamená, je povinný ich uschovať samostatne od ostatných dôverných údajov a na takom mieste, ktoré nie je voľne prístupné tretím osobám.
3. Klient je povinný neuvádzať dôverné údaje tak, aby sa dali spojiť s príslušným účtom (napr. napísanie dôverných údajov v dokladoch spojených s účtom, automatické zapamätanie prihlasovacieho mena a hesla do internetbankingu zariadením).
4. Klient je povinný dodržiavať dostatočnú mieru obozretnosti pri správe dôverných údajov, predovšetkým nezadávať dôverné údaje pred inou osobou, neoznamovať dôverné údaje iným osobám, a to ani rodinným príslušníkom a blízkym osobám. Za porušenie týchto Podmienok sa však nepovažuje oznámenie užívateľského mena inej fyzickej osobe za účelom zriadenia oprávnenia k účtu tejto osoby, resp. k účtu ovládanému touto osobou.
5. Klient je povinný si zvoliť heslo ako kombináciu čísiel a veľkých a malých písmen, bez osobného vzťahu k svojej osobe či k blízkym osobám. Jednoduché heslo s osobnými rysmi je ľahšie odhaliteľné. Klient nesmie použiť ako heslo a PIN pre smartbanking svoj dátum narodenia, rodné číslo, telefónne číslo, po sebe idúce číslice apod. Klient je povinný heslo a PIN pre smartbanking pravidelne meniť. Nikdy nemeňte heslo do internetbankingu na inom formulári, než v záložke Globálne nastavenia v internetbankingu. Banka nebude v žiadnom prípade vyžadovať od klienta iný postup. Prvé heslo je klient povinný si zmeniť pri prvom prihlásení do internetbankingu. Platnosť nasledujúceho hesla je z bezpečnostných dôvodov obmedzená na 365 dní. Ak vyprší uvedené lehota, bude klient pri najbližšom prihlásení do internetbankingu vyzvaný k zmene hesla.
6. Klient je povinný dodržiavať dostatočnú mieru obozretnosti pri zadávaní dôverných údajov, predovšetkým nezasielať dôverné údaje pomocou e-mailu alebo sms, nezadávať ich na inej internetovej stránke, než na stránke určenej na prihlasovanie do internetbankingu, a to ani v prípade, ak klient obdrží e-mail či sms, ktorá napodobňuje výzvu, najmä od Banky, na zaslanie dôverných údajov alebo na ich vyplnenie na inej internetovej stránke. Banka takýto druh správ v žiadnom prípade nebude posielať svojim klientom.

Čl. XII. Uloženie elektronického kľúča

1. Klient je povinný chrániť svoj elektronický kľúč, ktorý používa pri zadávaní pokynov, proti jeho zneužitiu, najmä proti jeho odcudzeniu, skopírovaniu a pod. Zneužitím elektronického kľúča klienta môže iná osoba predstierať identitu klienta a zadávať pokyny v mene klienta. Zneužitie elektronického kľúča môže spôsobiť klientovi škodu.
2. Klient je povinný inštalovať elektronický kľúč iba na počítač, o ktorom si môže byť s dostatočnou mierou istý, že je chránený pred možnými hrozbami plynúcimi z pripojenia k dátovej sieti. Klient nesmie inštalovať a používať elektronický kľúč na počítač, ktorý je verejne prístupný.

3. Ak klient uchováva elektronický kľúč na inom prenosnom médiu, je povinný toto médium uložiť na miesto, kde je do veľkej miery obmedzené riziko jeho zneužitia, najmä odcudzenia, skopírovania či poškodenia.

Čl. XIII. Bezpečnostné opatrenia vo sfére vplyvu klienta, zabezpečenie zariadenia klienta

1. Klient je povinný dodržiavať všetky povinnosti, ktoré sú stanovené v ods. 2 až 12 tohto článku. Všetky informácie obsiahnuté v ods. 2 až 12 tohto článku sú pre klienta povinnosťami.
2. Klient je povinný používať internetbanking iba na zariadeniach, ktoré sú riadne zabezpečené proti zneužitiu dôverných údajov. Klient nesmie používať internetbanking hlavne v internetových kaviarňach a na iných verejne prístupných zariadeniach, ani na zariadeniach, u ktorých klient nemá dostatočnú mieru istoty, že sú zabezpečené proti zneužitiu dôverných údajov. Klient je povinný používať internetbanking len na takých zariadeniach, pri ktorých si môže byť s dostatočnou mierou istý práv, ktoré má nastavené ako užívateľ takéhoto zariadenia a práv, ktoré majú tretie osoby nastavené k tomuto zariadeniu, vrátane práv umožňujúcich diaľkový prístup.
3. Klient je povinný sa pred prihlásením do internetbankingu riadne presvedčiť, že komunikuje so správnym poskytovateľom služby. Klient je povinný vždy si overiť, že vstupná stránka má v prehliadači jednu z týchto adries: www.fio.sk, www.fio.cz, www1.fio.cz, www2.fio.cz, www3.fio.cz, www.fiobanka.com, www.fio.hu, www.e-broker.cz, ib.fio.cz, ib.fio.sk. Banka má právo kedykoľvek obmedziť prístup na ktorýkoľvek zo serverov Banky, a to dočasne aj natrvalo.
4. Klient je povinný pri prihlasovaní sa do aplikácie internetbanking a pri zadávaní pokynov prostredníctvom aplikácie internetbanking riadne skontrolovať, že spojenie je zabezpečené (overiť platnosť certifikátu SSL zabezpečenia) a ďalej overiť identifikáciu servera Banky. Pri využívaní služieb Banky poskytovaných prostredníctvom internetu (predovšetkým Internetbanking a e-Broker) je kliet vždy povinný si skontrolovať, že komunikuje s Bankou šifrovanou komunikáciou (https) za použitia certifikátu SSL servera a ďalej je v uvedených prípadoch, pri každom svojom pripojení na server Banky, povinný overiť, či certifikát SSL servera je certifikátom s rozšíreným overením identity vydaným pre Fio banka, a.s. Praha 1 Česká republika, CZ, či certifikát SSL servera vydala spoločnosť GeoTrust Inc., či certifikát SSL servera je platný (neuplynul dátum platnosti) a tiež je povinný overiť identifikáciu certifikátu SSL servera (SHA1 Fingerprint) porovnaním so správnou identifikáciou, ktorá je dostupná na: http://www.fio.sk/docs/sk/fingerprint-sk.pdf. V prípade aplikácie smartbanking je klient povinný overiť identitu poskytovateľa a autora aplikácie pri jej inštalácii do mobilného zariadenia. Pri pripojení na server Banky prostredníctvom aplikácie smartbanking klient overenie identifikácie serveru Banky už nevykonáva. Banka nezodpovedá za škodu spôsobenú klientom porušením jeho povinností stanovených v tomto odseku.
5. Klient je pri každom svojom pripojení aplikáciou Fio-podpis (ďalej tiež „elektronický kľúč“) povinný overiť jej identifikáciu (SHA1 Fingerprint) porovnaním so správnou identifikáciou, ktorá je dostupná na: http://www.fio.sk/docs/sk/fingerprint-sk.pdf. Banka nezodpovedá za škodu spôsobenú porušením tejto povinnosti klientom. Identifikácia Fio-podpisu je zobrazená v okne prostredia JAVA pri spustení aplikácie Fio-podpis, alebo - v prípade prijatia tohto certifikátu za dôveryhodný – v dôveryhodných certifikátoch v prostredí JAVA.
6. Identifikácia podľa odseku 4 a 5 tohto článku je pravidelne menená. Z tohto dôvodu je klient povinný pri každom svojom pripojení na server Banky overiť aktuálnosť identifikácie. Jej správne a aktuálne znenie získa klient na: http://www.fio.sk/docs/sk/fingerprint-sk.pdf alebo na ktorejkoľvek pobočke Banky. Banka nezodpovedá za školu porušením tejto povinnosti klientom.
7. Klient má povinnosť v prípade akýchkoľvek pochybností o tom, že komunikuje s Bankou, alebo že spojenie nie je riadne zabezpečené, nevykonávať žiadne úkony, ktoré by mohli viesť k prezradeniu alebo zneužití dôverných údajov, predovšetkým prihlasovacích údajov a bezodkladne kontaktovať klientskeho pracovníka Banky.
8. Klient je povinný legálne zabezpečiť zariadenie, na ktorom sa rozhodne používať internetbanking, firewallom, antivírovou a anti- spywareovou ochranou, a tieto ochranné

prvky pravidelne aktualizovať. Klient je povinný aktualizovať programy štandardným spôsobom a pravidelne sledovať informácie o nových hrozbách, vírusoch, spywareoch a pod. a v súlade s tým zabezpečiť ochranu takého zariadenia.

9. Klient je povinný používať internetbanking iba na takých zariadeniach, na ktorých je legálne zaobstaraný a pravidelne aktualizovaný operačný systém. Klient je povinný pravidelne sledovať správy výrobcu operačného systému o opravách chýb a nedostatkov tohto operačného systému a tieto opravy včas inštalovať do zariadení, na ktorom je používaný internetbanking..
10. Klient je povinný používať dôveryhodný internetový prehliadač, ktorý pravidelne aktualizuje. Taktiež je povinný nastaviť zabezpečenie tohto prehliadača štandardným spôsobom a skontrolovať vždy pred zadaním prihlasovacích údajov, či internetový prehliadač nehlási akékoľvek varovanie, obzvlášť varovanie ohľadom dôveryhodnosti certifikátu SSL serveru. Klient je povinný na zariadeniach, na ktorých používa internetbanking vyvarovať sa sťahovaniu a inštalovaniu programov, ktoré možno voľne získať na internete, u ktorých si nemôže byť s dostatočnou mierou istý, že neobsahujú vírusy alebo spyware, prípadne že nepochádzajú zo zdroja, ktorý je nedôveryhodný. Klient je povinný na zariadeniach, na ktorých používa internetbanking navštevovať iba známe, dôveryhodné a bezpečné stránky na internete a neotvárať nevyžiadané emaily, emaily od neznámych odosielateľov a emaily s podozrivým názvom alebo obsahom na takýchto zariadeniach. Takéto emaily je klient povinný bez otvorenia vymazať. Klient je povinný vo svojej emailovej schránke používať spam filter.
11. Banka upozorňuje klienta, že žiadne licenčné podmienky pri voľne šírenom software nemôžu klientovi poskytnúť istotu, že software neobsahuje súčasti, ktoré môžu zariadenie klienta poškodiť či inak narušiť bezpečnosť ukladaných údajov klienta.
12. Vyspelejšie mobilné zariadenia (najmä tzv. smartphony a tablety) s operačným systémom iOS, Android, Windows Phone a podobným operačným systémom, je nevyhnutné chrániť obdobne ako počítač, a to prostredníctvom legálneho antivirového programu; je taktiež žiadúce neinštalovať aplikácie z iných než oficiálnych zdrojov pre príslušný operačný systém mobilného zariadenia (napr. Apple App Store, Google Play, Window Phone Store, atď.) banka však upozorňuje, že klient nemôže spoliehať na kontrolu vykonávanú prevádzkovateľom operačného systému vo vzťahu ku všetkým aplikáciám. Klient je povinný legálne zabezpečiť takéto mobilné zariadenie, na ktorom sa rozhodne používať internetbanking firewallom, antivírovou a anti-spywareovou ochranou, a tieto ochranné prvky pravidelne aktualizovať. Klient je v náväznosti na to povinný aktualizovať programy štandardným spôsobom, pravidelne sledovať informácie o nových hrozbách, vírusoch, spywareoch a pod. a v súlade s tým prispôsobovať ochranu mobilného zariadenia.
13. Banka odporúča klientovi, aby pred každým zadaním dôveryhodných údajov si overil, že zariadenie, z ktorého sa hlási, používa DNS prehliadače podporujúce DNSSEC a prehliadač si nastavil tak, aby sám vedel vykonávať DNSSEC overovanie.
14. Banka odporúča klientovi priebežne sa oboznamovať s aktuálnymi informáciami o možnostiach zabezpečenia zariadenia a o aktuálnych rizikách, ktoré pri používaní zariadenia hrozí. V prípade, ak klientove znalosti tejto problematiky nie sú na riadne zabezpečenie zariadení dostačujúce, resp. ak sám klient má o ich dostatočnosti pochybnosti, Banka odporúča klientovi obrátiť sa s požiadavkou na zabezpečenie zariadenia a jeho prípadného komunikačného príslušenstva na odborníka.

Čl. XIV. Zabezpečenie sms a mobilného zariadenia

1. Pre prijímanie autorizačných sms kódov je najdôležitejšia SIM karta, ktorá obsahuje telefónne číslo, ktoré ste určili na prijímanie autorizačných sms kódov od Banky (ďalej len „SIM karta“). Mobilné zariadenie bez SIM karty neumožní komunikáciu s Bankou a autorizáciu.
2. Klient je povinný mať mobilné zariadenie či SIM kartu pod dohľadom a neponechávať ich ležať na miestach, kde nad nimi nemá kontrolu.

3. Klient je povinný vyvarovať sa požičiavaniu mobilného zariadenia či SIM karty tretím osobám bez toho, aby ste mal neustálu kontrolu nad ich nakladaním s mobilným zariadením a SIM kartou.
4. V prípade, že hrozí riziko, že by klient mohol ponechať mobilné zariadenie mimo svoj dohľad, je povinný znemožniť jeho používanie tretím osobám kódom PIN a tento kód uchovávať v tajnosti a neoznamovať ho tretím osobám, ani si ho nikam nepoznamenávať.
5. Autorizačný kód, ktorý klientovi je doručený Bankou, si klient nesmie nikam poznamenávať a sms s autorizačným kódom nesmie žiadnej osobe sprístupňovať.
6. Klient je povinný v závislosti od technického pokroku v oblasti funkcií mobilných zariadení zabezpečiť funkcie svojho mobilného zariadenia proti možnosti automatického pripojenia tretej osoby k mobilnému zariadeniu.
7. Pre smartbanking a autorizáciu využitím aplikácie smartbanking je najdôležitejšie mobilné zariadenie, ktorého UID klient určil pre tento druh služby. Klient je povinný mať takéto mobilné zariadenie vždy pod dohľadom. Pre jeho zabezpečenie platia obdobne pravidlá pre mobilné zariadenia uvedené vyššie. Klient je povinný sa vždy odhlásiť z aplikácie smartbanking bezprostredne po ukončení práce s ňou a nikdy nepožičiavať ani neponechávať mimo dohľad svoje mobilné zariadenie, pokiaľ je prihlásený do aplikácie smartbanking.
8. I v prípade, že na mobilnom zariadení klient nepoužíva internetbanking ani smartbanking, ale v takomto mobilnom zariadení je zapojená SIM karta (tzn. SIM karta, ktorá obsahuje telefónne číslo, ktoré je určené k prijímaniu autorizačných sms kódov od banky), je klient povinný zabezpečiť takéto mobilné zariadenie legálnym firewallom, antivírovou a anti-spywareovou ochranou a tieto ochranné prvky pravidelne aktualizovať. Klient je povinný aktualizovať programy štandardným spôsobom a pravidelne sledovať informácie o nových hrozbách, víroch, spywareoch apod. a v súlade s tým zaistiť ochranu takéhoto zariadenia. Postup uvedený v tomto odseku slúži k obmedzeniu rizika utajeného preposielania autorizačných sms kódov zasielaných Bankou (v prípade napadnutého mobilného zariadenia); alternatívou k obmedzeniu uvedeného rizika je používanie SIM karty výlučne v tzv. „hlúpych“ telefónoch.

Čl. XIVa. Blokácia internetbankingu a smartbankingu

1. Banka je oprávnená trvalo alebo dočasne zablokovať internetbanking v prípade, že:
a) vznikne podozrenie na zneužitia internetbankingu alebo dôjde k zneužitiu internetbankingu,
b) sa významne zvýši riziko, že klient nebude schopný splácať úver, ktorý možno čerpať prostredníctvom internetbankingu.
2. Banka je oprávnená trvalo alebo dočasne zablokovať smartbanking v prípade, že vznikne podozrenie zo zneužitia smartbankingu alebo dôjde k zneužitiu smartbankingu.
3. Banka je oprávnená trvalo alebo dočasne zablokovať použitie biometrického snímača pre aplikáciu smartbanking v mobilnom zariadení v prípade, že vznikne podozrenie zo zneužitia alebo dôjde ku zneužitiu tohto spôsobu autorizácie.

Čl. XV. Kontaktujte klientskeho pracovníka

1. V prípade, že klient obdrží e-mail s upozornením na akúkoľvek zmenu v spôsobe prihlasovania do internetbankingu či s informáciou o zmene www adresy prihlasovacej stránky, alebo v prípade, že klient zistí netypické či inak podozrivé správanie sa prihlasovacej stránky, vrátane automatického presmerovania, alebo iné podozrivé skutočnosti, klient nesmie vykonávať žiadne úkony, ktoré by mohli viesť k prezradeniu či k zneužitiu dôverných údajov a je povinný bezodkladne kontaktovať pracovníkov Banky.

Čl. XVI. Oznámenie o zneužití internetbankingu a smartbankingu

1. Klient je povinný bezodkladne oznámiť Banke stratu, odcudzenie alebo zneužitie prihlasovacieho mena a hesla do internetbankingu či smartbankingu, neautorizovaný prístup do smartbankingu pomocou biometrických údajov, elektronického podpisu, mobilného

zariadenia (SIM karty), na ktoré sa zasielajú sms kódy, mobilného zariadenia s aplikáciou smartbanking alebo iných dôverných údajov, ako aj iné zneužitie alebo neautorizované použitie internetbankingu či smartbankingu.

2. Klient je povinný oznámiť stratu, odcudzenie alebo zneužitie vyššie uvedených údajov a iné zneužitie či neautorizované použitie internetbankingu či smartbankingu telefonicky na tel. číslo: +421 2 5262 0990. Táto telefónna linka je klientovi k dispozícii nepretržite ktorýkoľvek deň v roku. Pri oznámení je klient povinný uviesť aspoň tieto údaje: osobné identifikačné údaje a svoje prihlasovacie meno do internetbankingu. Bez oznámenia týchto údajov sa nepovažuje oznámenie klienta za riadne a Banka nie je povinná takéto oznámenie prijať. V prípade riadneho oznámenia je Banka oprávnená, ale nie povinná, overiť toto oznámenie napr. spätným kontaktovaním klienta. Klient súhlasí s tým, že Banka je oprávnená z preventívnych a bezpečnostných dôvodov od okamžiku riadneho prijatia oznámenia podľa tohto článku nevykonávať žiadne už podané alebo už prijaté pokyny na ťarchu účtu, ku ktorému má klient prístup na základe oznámeného prihlasovacieho mena do internetbankingu a zablokovať prístup do internetbankingu na základe tohto užívateľského mena. Banka nie je zodpovedná za škodu spôsobenú klientovi z dôvodu vykonania bezpečnostných opatrení podľa tohto článku.

Čl. XVIa. Informácie o poskytovaní finančného sprostredkovania

1. Pri uzatváraní zmlúv a ďalších súvisiacich právnych úkonoch je Banka, pokiaľ z predmetného právneho úkonu nevyplýva inak, zastúpená obchodnou spoločnosťou Fio Slovakia, a.s., IČO: 35 828 137, so sídlom Nám. SNP 21, 811 01 Bratislava, zapísanou v obchodnom registri vedenom Okresným súdom Bratislava I., oddiel: Sa, vložka č.: 2892/B (ďalej aj len „finančný sprostredkovateľ“). Finančný sprostredkovateľ je akciovou spoločnosťou.
2. Finančný sprostredkovateľ je odo dňa 23.10.2015 pod registračným číslom 208336 zapísaný v Registri finančných agentov a finančných poradcov vedenom Národnou bankou Slovenska, dostupnom na webovej stránke https://regfap.nbs.sk/, ako viazaný finančný agent pre sektor poskytovania úverov a spotrebiteľských úverov a pre sektor prijímania vkladov a ako viazaný investičný agent pre sektor kapitálového trhu. Registráciu je možné overiť si na uvedenej webovej stránke.
3. Finančný sprostredkovateľ vykonáva finančné sprostredkovanie na základe písomnej mandátnej zmluvy výhradnej povahy, ktorú má uzatvorenú s jednou finančnou inštitúciou – Bankou. Finančný sprostredkovateľ je z titulu tejto zmluvy oprávnený zastupovať Banku pri uzatváraní zmluvy s klientom a k ďalším právnym úkonom v rámci zmluvného vzťahu s klientom. Odplatu za vykonávanie finančného sprostredkovania hradí Banka. Na žiadosť klienta bude jej výška oznámená. Finančný sprostredkovateľ vykonáva finančné sprostredkovanie v súlade s touto zmluvou a v súlade so zákonom č. 186/2009 Z.z. o finančnom sprostredkovaní a finančnom poradenstve a o zmene a doplnení niektorých zákonov.
4. Finančný sprostredkovateľ nemá kvalifikovanú účasť na základnom imaní ani hlasovacích právach Banky. Banka má kvalifikovanú účasť na základnom imaní a hlasovacích právach finančného sprostredkovateľa. Banka je jediným spoločníkom českej obchodnej spoločnosti RM-S FINANCE, s.r.o., IČO: 629 15 240 sídlo: Česká republika, 117 21 Praha 1, V Celnici 1028/10. Obchodná spoločnosť RM-S FINANCE, s.r.o. je jediným akcionárom finančného sprostredkovateľa.
5. Osobitnými predpismi upravujúcimi mimosúdne riešenie sporov vyplývajúcich z finančného sprostredkovania sú najmä zákon č. 244/2002 Z.z. o rozhodcovskom konaní, zákon č. 355/2014 Z.z. o spotrebiteľskom rozhodcovskom konaní a o zmene a doplnení niektorých zákonov, zákon č. 420/2004 Z.z. o mediácii a o doplnení niektorých zákonov a zákon č. 391/2015 Z.z. o alternatívnom riešení spotrebiteľských sporov a o zmene a doplnení niektorých zákonov.
6. Klient je oprávnený podať reklamáciu (sťažnosť) na vykonávanie finančného sprostredkovania Banke alebo finančnému sprostredkovateľovi v súlade s Reklamačným

poriadkom Banky. Ďalšie podrobnosti sú uvedené v Reklamačnom poriadku zverejnenom na webovej stránke www.fio.sk.

7. Poplatky a iné náklady finančnej služby, ktoré hradí klient, sú uvedené v príslušnom Cenníku Banky. Finančnému sprostredkovateľovi klient Banky neplatí žiadnu odmenu.

Čl. XVII. Záverečné ustanovenia

1. V záujme zlepšenia kvality služieb poskytovaných klientovi, v súvislosti so zmenou identifikácie (fingerprintu) serveru Banky, v nadväznosti na vývoj právneho prostredia a tiež s ohľadom na obchodnú politiku Banky je Banka oprávnené tieto Podmienky meniť a dopĺňať (vyhlasovať nové znenie). Banka je oprávnená navrhnúť klientovi zmenu zmluvy o elektronickej správe účtu a týchto obchodných podmienok (ďalej tiež „návrh na zmenu zmluvy“). Návrh na zmenu zmluvy sa klientovi poskytuje aspoň 2 mesiace pred navrhovaným dňom účinnosti zmeny, a to prostredníctvom internetbankingu. Zmluvné strany sa dohodli, že ak klient pred navrhovaným dňom účinnosti návrhu na zmenu zmluvy neoznámi Banke, že návrh na zmenu zmluvy neprijíma, platí, že klient návrh na zmenu zmluvy prijal. Ak klient nesúhlasí s návrhom na zmenu zmluvy, má právo na okamžité ukončenie zmluvy o elektronickej správe účtov bez poplatkov pred navrhovaným dňom účinnosti návrhu na zmenu zmluvy. Ak klient oznámi Banke, že s návrhom na zmenu zmluvy nesúhlasí, považuje sa to automaticky za výpoveď zmluvy o elektronickej správe účtov podanú Bankou, ak Banka nestanoví inak. Oznámenie o nesúhlase klienta s návrhom na zmenu zmluvy, odvolanie tohto oznámenia, uplatnenie si práva na okamžité ukončenie zmluvy, ako aj prípadná výpoveď zmluvy zo strany klienta musia byť doručené Banke v písomnej podobe na adresu jej sídla či príslušnému pracovisku (pobočke). Ak bola podaná výpoveď zmluvy, klient je oprávnený pred uplynutím výpovednej doby a pred navrhovaným dňom účinnosti návrhu na zmenu zmluvy odvolať svoj nesúhlas s návrhom na zmenu. Včasné odvolanie nesúhlasu s návrhom na zmenu zmluvy, podľa predchádzajúcej vety, má za následok, že podaná výpoveď sa považuje za zrušenú. Klient žiada Banku, aby mu bol návrh na zmenu zmluvy alebo obchodných podmienok zaslaný prostredníctvom internetbankingu do tejto aplikácie v podobe nového úplného znenia zmluvy či obchodných podmienok tak, aby mohol tento návrh uchovať a využívať počas primeranej doby a aby mohol tento návrh v nezmenenej podobe reprodukovať. Banka žiadosť klienta prijíma.
2. Tieto Podmienky boli vyhlásené dňa 1.7.2016, nadobúdajú účinnosť dňa 4.7.2016 a k rovnakému dňu nahrádzajú všetky doterajšie Obchodné podmienky pre elektronickú správu účtov, ak nie je ďalej uvedené inak. Vo vzťahu k zmluvám uzatvoreným predo dňom nadobudnutia účinnosti Podmienok podľa predchádzajúcej vety, nadobúdajú Podmienky účinnosť dňa 2.9.2016 a k rovnakému dňu nahrádzajú doterajšie Obchodné podmienky pre elektronickú správu účtov.

Ing. Marek Polka v. r.
vedúci organizačnej zložky