OBCHODNÍ PODMÍNKY BANKY CREDITAS a.s. PRO INTERNETOVÉ BANKOVNICTVÍ

ÚČINNÉ OD ~~8. 1. 2024~~1. 10. 2024

OBSAH

1 ÚVODNÍ USTANOVENÍ

1.1 Úvod

1.1.1 Tyto Obchodní podmínky pro Internetové bankovnictví (dále jen **„OP“**) vydává Banka CREDITAS a.s. (dále jen „**Banka**“) v souladu se Všeobecnými obchodními podmínkami Banky (dále jen **„VOP“**). Tyto OP představují Obchodní podmínky ve smyslu VOP.

1.1.2 Tyto OP stanovují další konkrétní pravidla a podmínky upravující vztahy mezi Bankou a Klientem související s poskytováním služeb Internetového bankovnictví. Skutečnosti týkající se Internetového bankovnictví, které nejsou v těchto OP upravené, se řídí příslušnými ustanoveními VOP, Sdělení k platebním službám a provádění platebního styku (dále jen „**Sdělení**“), Občanského zákoníku a dalších souvisejících právních předpisů.

1.1.3 Tyto OP tvoří v souladu s § 1751 Občanského zákoníku na základě odkazu část obsahu každé Smlouvy, na základě které jsou Bankou Klientovi poskytovány služby Internetového bankovnictví, a tudíž jsou její nedílnou součástí. Klient je povinen se s těmito OP seznámit a dodržovat je.

1.2 Vymezení pojmů a výkladová pravidla

1.2.1 Pokud z kontextu těchto OP nevyplývá něco jiného, mají pojmy s velkým počátečním písmenem či jiné pojmy používané v těchto OP, které se vztahují na jednotná i množná čísla těchto pojmů, nevyplývá-li z kontextu jinak, význam stanovený ve VOP nebo jinde v textu těchto OP nebo význam níže uvedený:

„Bankovní identitou“ se rozumí služba poskytovaná Bankou spočívající v možnosti využití přihlašovacího jména a personalizovaných bezpečnostních prvků Uživatele používaných v kombinaci pro přístup do Internetového bankovnictví také pro účely vydání prostředku pro elektronickou identifikaci a poskytování identifikačních služeb (např. prokázání totožnosti Uživatele na dálku) v souladu se ZEI a ZOB, a to vůči státním orgánům a orgánům územního samosprávného celku a umožňuje-li to Banka, také vůči jiným orgánům a soukromým poskytovatelům služeb.

„Dispozičním oprávněním“ se rozumí formulář Banky či jiný dokument akceptovaný ze strany Banky, v rámci kterého Klient zmocnil určitou fyzickou osobu nebo společně určité fyzické osoby k právnímu jednání vůči Bance vztahujícímu se k určité Finanční službě vedené Bankou na jméno tohoto Klienta nebo pro něj, a to prostřednictvím Internetového bankovnictví. Klient, který je fyzickou osobou, může prostřednictvím formuláře Dispozičního oprávnění měnit i své oprávnění k obsluze určité Finanční služby vedené Bankou na jeho jméno nebo pro něj prostřednictvím Internetového bankovnictví, kdy toto oprávnění je při zřízení takové Finanční služby automaticky nastaveno Klientovi jako plné oprávnění, které Internetové bankovnictví v danou chvíli umožňuje, a Banka se tímto nastavením Klienta řídí, pokud je z její strany Dispoziční oprávnění akceptováno.

„Informováním o platebním účtu“ se rozumí předávání informací o Platebním účtu Klientovi prostřednictvím třetí strany – oprávněného poskytovatele služby informování o platebním účtu; nebo předávání informací o jiném Platebním účtu Klienta, než který je vedený Bankou, Klientovi prostřednictvím Banky jako poskytovatele služby Informování o platebním účtu.

„Internetovým bankovnictvím“ se rozumí Finanční služba poskytovaná Bankou Klientovi spočívající v možnosti obsluhy Účtů či jiných produktů, resp. jiných Finančních služeb nabízených Bankou, Klientem a kontaktu Klienta s Bankou pomocí prostředků komunikace na dálku, a to v souladu s těmito OP a dalšími dokumenty vydanými Bankou upravujícími podmínky poskytování Internetového bankovnictví. Internetové bankovnictví poskytuje Banka Klientům prostřednictvím následujících aplikací:

a) **„CREDITAS Banking“** je ~~nová~~ webová aplikace v rámci Internetového bankovnictví;

b) **„CREDITAS Banking Mobile“** je ~~nová~~ mobilní aplikace Banky v rámci Internetového bankovnictví;

c) **„CREDITAS Invest App“** je mobilní aplikace Banky v rámci Internetového bankovnictví sloužící výlučně k poskytování Bankou vybraných investičních služeb.

„Manuálem k IB“ se rozumí jakýkoliv manuál či příručka, nebo jinak nazvaný materiál vydaný či připravený Bankou v jakékoliv formě (např. ve formátu *.pdf nebo formou videa) v souvislosti s Internetovým bankovnictvím a/nebo Bankovní identitou zejména za účelem zprostředkovat Uživatelům podrobný návod k bezpečnému využívání Internetového bankovnictví a/nebo Bankovní identity. Manuál k IB Banka zveřejňuje na svých Internetových stránkách a není Smluvním dokumentem ve smyslu VOP, tudíž je Banka oprávněna jej kdykoliv měnit. Manuálem k IB se rozumí i jakékoliv pokyny či instrukce Banky, které Uživatel vidí při přihlašování se do Internetového bankovnictví nebo již v prostředí Internetového bankovnictví a které Uživatele zejména instruují k tomu, jak správně postupovat, aby mohl být jím zadávaný požadavek správně proveden.

„NIA“ se rozumí Národní bod pro identifikaci a autentizaci v souladu se ZEI.

„Nepřímým dáním platebního příkazu“ se rozumí podání Platebního příkazu Klientem Bance prostřednictvím třetí strany – oprávněného poskytovatele služby nepřímého dání platebního příkazu; nebo podání Platebního příkazu pro jiný Platební účet Klienta, než který je vedený Bankou, Klientem prostřednictvím Banky jako poskytovatele služby nepřímého dání platebního příkazu.

„Registrovaným ČMT“ se rozumí číslo mobilního telefonu aktivované v síti libovolného operátora uvedené ve Smlouvě k IB uzavřené mezi Bankou a Uživatelem, které bude Banka používat ve vztahu k Internetovému bankovnictví využívanému

Uživatelem za účelem autentizace tohoto Uživatele, autorizace transakcí a operací prováděných tímto Uživatelem v rámci Internetového bankovnictví v souladu s těmito OP a podpis smluvních dokumentů a jiných příkazů a žádostí tohoto Uživatele v Internetovém bankovnictví. Změnu Registrovaného ČMT může Uživatel provést na základě písemné žádosti doručené osobně na jakoukoliv Pobočku Banky, případně prostřednictvím Internetového bankovnictví, pokud to Banka v daném případě umožňuje.

„Silným ověřením“ se rozumí ověření, které je založeno na použití alespoň 2 z těchto personalizovaných bezpečnostních prvků:

a) údaje, který je znám pouze Klientovi (přihlašovací heslo, MPIN),

b) věci, kterou má Klient ve své moci (přihlašovací SMS kód nebo autorizační SMS kód zasílaný na Registrované ČMT, případně samotný mobilní telefon registrovaný Bankou pro využívání příslušné aplikace v rámci Internetového bankovnictví),

c) biometrických údajů Klienta (otisk prstu nebo obličej Klienta).

„Smlouvou o IB“ se rozumí Smlouva o zřízení a vedení Internetového bankovnictví, kterou Banka uzavírá s Klientem.

„Uživatelem“ se rozumí fyzická osoba, se kterou Banka uzavřela Smlouvu o IB.

„ZEI“ se rozumí zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů.

1.2.2 Výkladová pravidla Smluvních dokumentů vydávaných Bankou, tj. zejména VOP, Obchodních podmínek, Sdělení a Sazebníku, jsou stanovena v odstavci 1.4 VOP.

2 INTERNETOVÉ BANKOVNICTVÍ

2.1 Obecné podmínky využívání Internetového bankovnictví (Smlouva o IB)

2.1.1 Banka zřídí pro Klienta Internetové bankovnictví a umožní mu jeho využívání ve vztahu k Finančním službám poskytovaným mu Bankou, u kterých to umožňuje, na základě Smlouvy o IB uzavřené mezi Bankou a Klientem na dobu neurčitou a příslušných platných Dispozičních oprávnění. Banka Internetové bankovnictví umožňuje zřídit

a) fyzickým osobám nepodnikajícím;

b) fyzickým osobám podnikajícím a

c) právnickým osobám.

2.1.2 Klientovi, který je fyzickou osobou, jež ještě nenabyla plné svéprávnosti, umožňuje Banka zřídit Internetové bankovnictví od věku 6 let, přičemž pro právní jednání takového Klienta platí podmínky stanovené VOP. Klient, který byl při uzavření Smlouvy o IB jakožto nezletilý zastoupen svým zákonným zástupcem a nepředložil Bance svůj doklad totožnosti, je povinen jej před dovršením zletilosti Bance předložit a podrobit se provedení řádné identifikace ve smyslu VOP. Nesplní-li Klient tuto povinnost nejpozději 2 měsíce před dovršením 18 let věku, může Banka odmítnout poskytnutí Finančních služeb, případně může od Smlouvy o IB odstoupit s okamžitou účinností. Klient a Banka se dohodli, že v případě nesplnění identifikační povinnosti podle tohoto ustanovení závazky ze Smlouvy o IB zaniknou poslední Obchodní den před dovršením 18 let věku Klienta, nebude-li Smlouva o IB ukončena dříve jiným způsobem. Při uzavření Smlouvy o IB Distančním způsobem musí být Klient mladší 18 let zastoupen rodičem; rodičem se pro účely těchto OP rozumí zákonný zástupce Klienta, který je uveden v rodném listě Klienta a kterému nebyla omezena rodičovská zodpovědnost ani mu nezaniklo právo pečovat o jmění dítěte.

2.1.3 Klient, který je fyzickou osobou, a má zájem o obsluhu Finančních služeb mu poskytovaných Bankou prostřednictvím Internetového bankovnictví, uzavírá s Bankou Smlouvu o IB s tím, že obsluhu příslušných Finančních služeb prostřednictvím Internetového bankovnictví může provádět Klient sám nebo jiní Uživatelé, které k tomu tento Klient zmocnil v rámci příslušných Dispozičních oprávnění a kteří s Bankou uzavřou samostatnou Smlouvu o IB. Smlouvu o IB je možné uzavřít:

a) na Pobočce nebo

b) Distančním způsobem prostřednictvím Žádosti na dálku ve smyslu VOP, pokud to Banka ve vztahu k dané osobě umožňuje.

2.1.4 Postup uzavření Smlouvy o IB Distančním způsobem v případě nezletilých Klientů, pokud jej Banka umožňuje prostřednictvím příslušné aplikace Internetového bankovnictví, je následující:

a) rodič Klienta prostřednictvím svého Internetového bankovnictví vyplní Žádost na dálku o založení produktů Klienta podle konkrétních pokynů uvedených v Internetovém bankovnictví;

b) rodič Klienta doloží identifikační údaje a rodný list Klienta, přičemž:

   i. pořídí barevnou fotografii originálu rodného listu v rámci Žádosti na dálku, a to v takové kvalitě, aby byly příslušné údaje čitelné a úplné; v tomto rodném listě musí být rodič Klienta zapsán jako matka nebo otec Klienta;

   ii. Banka je oprávněna požadovat opětovné doložení rodného listu, případně jiného dokladu;

c) rodič Klienta se seznámí se zněním Smlouvy o IB a smlouvy k příslušnému produktu (dále jen „**Smlouvy**“), příslušnými Obchodními podmínkami, případně další poskytnutou smluvní dokumentací k zakládaným produktům, následně podepíše Smlouvy způsobem stanoveným Bankou;

d) Banka poskytne Klientovi, resp. rodiči Klienta, podepsané dokumenty a související smluvní dokumentaci v textové podobě ve formátu neumožňujícím změnu jeho obsahu, prostřednictvím e-mailu, který byl pro komunikaci s Bankou zvolen;

e) Žádost na dálku musí být dokončena a Smlouvy podepsány do 45 dnů od zahájení Žádosti na dálku, jinak bude celá Žádost

na dálku zrušena, nebylo-li dohodnuto jinak. Klient bere na vědomí a souhlasí s tím, že Banka může i po podpisu Smluv Žádost na dálku zamítnout, o čemž bude Klienta neprodleně informovat; zamítnutím Žádosti na dálku se má za to, že Banka od Smluv odstoupila, nebylo-li dohodnuto jinak.

2.1.5 Klient, který je právnickou osobou, a má zájem o obsluhu Finančních služeb mu poskytovaných Bankou prostřednictvím Internetového bankovnictví, uzavírá s Bankou Smlouvu o IB s tím, že bere na vědomí, že samotnou obsluhu příslušných Finančních služeb prostřednictvím Internetového bankovnictví mohou provádět pouze Uživatelé, které k tomu tento Klient zmocnil v rámci příslušných Dispozičních oprávnění a kteří s Bankou uzavřou samostatnou Smlouvu o IB.

2.1.6 Banka na základě Smlouvy o IB umožní Uživateli prostřednictvím Internetového bankovnictví obsluhu těch Finančních služeb,

a) které jsou vedeny na jméno tohoto Uživatele nebo pro něj, a to v rozsahu, ve kterém to Banka umožňuje, uvedené za předpokladu, že Uživatel obsluhu příslušné Finanční služby neomezil v rámci Dispozičního oprávnění;

b) které jsou vedeny na jméno jiného Klienta nebo pro tohoto jiného Klienta, a to v rozsahu, ve kterém to Banka umožňuje, pokud k obsluze daných Finančních služeb prostřednictvím Internetového bankovnictví tento jiný Klient Uživatele zmocní v rámci příslušných Dispozičních oprávnění, a to v rozsahu dle těchto Dispozičních oprávnění.

2.1.7 Za účelem vyloučení všech pochybností se uvádí, že Banka umožní obsluhovat konkrétním Uživatelům prostřednictvím Internetového bankovnictví automaticky i ty Finanční služby, jejichž poskytování bylo mezi Bankou a Klientem sjednáno až po uzavření Smlouvy o IB, za podmínek uvedených v bodě 2.1.6.

2.1.8 Dojde-li z jakéhokoliv důvodu k ukončení závazků ze Smlouvy o IB uzavřené mezi Bankou a Uživatelem, Banka automaticky zruší možnost využívání Internetového bankovnictví tímto Uživatelem.

2.1.9 Dojde-li z jakéhokoliv důvodu k ukončení závazků ze Smlouvy o IB uzavřené mezi Bankou a Klientem, Banka automaticky zruší možnost obsluhy všech Finančních služeb Klienta prostřednictvím Internetového bankovnictví všem Uživatelům, kteří byli k jejich obsluze zmocněni na základě příslušných Dispozičních oprávnění.

2.1.10 Dojde-li z jakéhokoliv důvodu k zneplatnění Dispozičního oprávnění Uživatele, Banka automaticky zruší možnost obsluhy odpovídajících Finančních služeb tímto Uživatelem prostřednictvím Internetového bankovnictví.

2.1.11 Banka automaticky zruší možnost obsluhy určité Finanční služby Klienta prostřednictvím Internetového bankovnictví Uživateli, který byl na základě příslušného Dispozičního oprávnění Klientem zmocněn k obsluze příslušné Finanční služby Klienta prostřednictvím Internetového bankovnictví pouze na dobu určitou či do doby existence určité právní události (např. do doby smrti Klienta), a to neprodleně po uplynutí stanovené doby nebo po prokázání existence příslušné právní události Bance.

2.1.12 Zrušení možnosti využívání Internetového bankovnictví určitým Uživatelem nebo možnosti obsluhy určité Finanční služby prostřednictvím Internetového bankovnictví konkrétním Uživatelem v souladu s body 2.1.8 až 2.1.11 těchto OP Banka provede nejpozději do konce následujícího Obchodního dne od právní skutečnosti rozhodné pro toto zrušení, pokud nebude v konkrétním případě mezi Bankou a Klientem dohodnuto jinak.

2.1.13 Závazky ze Smlouvy o IB uzavřené mezi Bankou a Klientem, který je fyzickou osobou, zaniknou v Rozhodný den (k tomu viz VOP) vztahující se k tomuto Klientovi, pokud nebude existovat žádné platné Dispoziční oprávnění udělené tímto Klientem jinému Uživateli nebo po Rozhodném dni vztahujícím se k tomuto Klientovi v den, kdy z jakéhokoliv důvodu pozbude platnosti poslední Dispoziční oprávnění udělené tímto Klientem jinému Uživateli. Banka zablokuje přístup do Internetového bankovnictví na základě personalizovaných bezpečnostních prvků konkrétního Uživatele v Rozhodný den vztahující se k tomuto Uživateli.

2.1.14 Závazky ze Smlouvy o IB uzavřené mezi Bankou a Klientem, který je právnickou osobou, zaniknou po zániku Klienta bez právního nástupce.

2.1.15 Závazky ze Smlouvy o IB mohou být Klientem vypovězeny s okamžitou účinností ke dni doručení výpovědi Bance, tj. bez výpovědní doby. Banka má právo závazky ze Smlouvy o IB vypovědět v souladu s VOP.

2.1.16 Od Smlouvy o IB může Banka odstoupit v souladu s VOP.

2.2 Využívání Internetového bankovnictví (autentizace a autorizace)

2.2.1 V rámci Internetového bankovnictví umožňuje Banka využívání aplikací CREDITAS Banking, CREDITAS Banking Mobile a CREDITAS Invest App.

2.2.2 Při využívání Internetového bankovnictví Banka vyžaduje Silné ověření Uživatele:

a) při přístupu (autentizaci) do příslušné aplikace Internetového bankovnictví,

b) při zadání (autorizaci) Platebního příkazu prostřednictvím Internetového bankovnictví nebo při Nepřímém dání platebního příkazu, za podmínek stanovených ve Sdělení,

c) při udělení souhlasu k využívání služby Informování o platebním účtu k Platebnímu účtu Klienta vedeného u Banky, za podmínek uvedených v těchto OP,

d) při provádění operací v Internetovém bankovnictví, které jsou spojeny s rizikem podvodu v oblasti platebního styku, zneužitím Platebního prostředku nebo informací o Platebním účtu (např. změna přihlašovacího hesla, změna PIN apod.),

e) v jiných případech vyžadovaných právními předpisy.

2.2.3 Aplikace CREDITAS Banking je Uživatelům přístupná prostřednictvím Internetových stránek Banky po provedení příslušné autentizace Uživatele ze strany Banky, tj. ověření a potvrzení totožnosti Uživatele Bankou, prostřednictvím zadání přihlašovacího jména, které si Uživatel zvolil při sjednání Smlouvy o IB a následujících společných personalizovaných bezpečnostních prvků:

a) přihlašovacího hesla Uživatele:
přihlašovací heslo pro první přihlášení Uživatele obdrží Uživatel na samostatném dokumentu neprodleně po uzavření Smlouvy o IB na Pobočce nebo si jej Uživatel zvolí sám při uzavírání Smlouvy o IB Distančním způsobem; Uživatel je povinen si přihlašovací heslo obdržené na samostatném dokumentu od Banky po prvním přihlášení do aplikace Internetového bankovnictví v jejím prostředí změnit; přihlašovací heslo musí být Uživatelem nastaveno v souladu s Manuálem k IB; Uživatel je oprávněn své přihlašovací heslo kdykoliv prostřednictvím příslušné aplikace změnit; a

b) přihlašovacího SMS kódu zaslaného Uživateli na Registrované ČMT:
přihlašovací SMS kód je unikátní kód, který Banka zasílá Uživateli na Registrované ČMT po zadání přihlašovacího jména v rámci prostředí Internetových stránek Banky určeného pro přihlášení do příslušné aplikace; platnost přihlašovacího SMS kódu je 3 minuty od jeho doručení na Registrované ČMT;
při další autentizaci Uživatele do příslušné aplikace Internetového bankovnictví může být kombinace přihlašovacího hesla a přihlašovacího SMS kódu nahrazena v aplikaci CREDITAS Banking – přihlášením prostřednictvím autentizace v aplikaci CREDITAS Banking Mobile po načtení přihlašovacího QR kódu.

2.2.4 K autorizaci operací v aplikaci CREDITAS Banking (zejména např. Platebních příkazů) dochází v závislosti na požadavku Banky a nastavení Uživatele prostřednictvím:

a) zadání autorizačního SMS kódu zaslaného na Registrované ČMT nebo
b) zadání kombinace přihlašovacího hesla a autorizačního SMS kódu nebo
c) potvrzením přes aplikaci CREDITAS Banking Mobile nebo
d) kliknutím na odpovídající potvrzovací tlačítko v aplikaci.

2.2.5 Minimální technické požadavky pro využívání aplikace CREDITAS Banking Uživatelem jsou následující:

a) osobní počítač nebo jiné obdobné zařízení (např. notebook, tablet) s připojením k internetu
b) aktuální verze podporovaného internetového prohlížeče
c) mobilní telefon.

2.2.6 Aplikace CREDITAS Banking Mobile je k dispozici volně ke stažení v App Storu,Google Play nebo v Huawei App Gallery, aplikace CREDITAS Invest App v App Storu a Google Play. Aplikace CREDITAS Banking Mobile musí být Uživatelem aktivována s využitím přihlašovacích údajů dle bodu 2.2.3 těchto OP. Aplikace CREDITAS Invest App musí být Uživatelem aktivována prostřednictvím webové aplikace CREDITAS Banking dle tam uvedených pokynů s využitím Bankou určeného personalizovaného bezpečnostního prvku Uživatele. Při aktivaci aplikací si Uživatel volí další personalizované bezpečnostní prvky (např. MPIN nebo možnost využívání biometrických údajů).

2.2.7 Pro autentizaci přístupu do aplikací CREDITAS Banking Mobile a CREDITAS Invest App, tj. pro ověření a potvrzení totožnosti Uživatele, je Bankou vyžadováno zadání MPIN nebo použití biometrických údajů Uživatele (např. otisk prstu, obličej Uživatele). K přístupu do aplikace CREDITAS Banking Mobile je možné využít i přihlašovací údaje dle bodu 2.2.3 těchto OP.

2.2.8 K autorizaci operací v aplikacích CREDITAS Banking Mobile (zejména např. Platebních příkazů) a CREDITAS Invest App dochází v závislosti na požadavku Banky a nastavení Uživatele prostřednictvím:

a) zadání MPIN nebo
b) zadání autorizačního SMS kódu zaslaného na Registrované ČMT (pouze v případě aplikace CREDITAS Invest App) nebo
c) použitím biometrických údajů nebo
d) kliknutím na odpovídající potvrzovací tlačítko v aplikaci.

V případě, že Banka umožňuje využívat pro autorizaci Platebních transakcí v aplikaci biometrické údaje a Uživatel má nastavenou možnost jejich využití, Banka automaticky nastavuje výchozí limit ve výši 5.000,- Kč či ekvivalent v cizí měně na autorizaci jednotlivé Platební transakce. Uživatel si může tento limit v aplikaci změnit.

2.2.9 Minimální technické požadavky pro využívání aplikací CREDITAS Banking Mobile a CREDITAS Invest App Uživatelem jsou následující:

a) chytrý mobilní telefon (podporované systémy iOS, Android) s připojením k internetu.

2.2.10 Počet zařízení, na kterých může jeden Uživatel provést aktivaci aplikace CREDITAS Banking Mobile nebo aplikace CREDITAS Invest App, může být omezen.

2.2.11 Uživatel je povinen zajistit, aby prostřednictvím Internetového bankovnictví komunikoval s Bankou pouze sám, tj. je povinen zamezit jiným osobám použití zařízení a aplikací, které využívá k přístupu do Internetového bankovnictví. V případě, že Uživatel využívá dle svého nastavení k autentizaci či autorizaci biometrických údajů, je povinen zajistit, že v příslušném zařízení má registrovány pouze své biometrické údaje, a dále je povinen neumožnit třetí osobě registrovat ve stejném zařízení její biometrické údaje.

2.2.12 Komunikačním jazykem je v rámci Internetového bankovnictví jazyk český, nebo jiný dle volby Uživatele, pokud takovouto volbu Banka Uživateli v rámci Internetového bankovnictví umožňuje.

2.2.13 Služby Internetového bankovnictví jsou Uživatelům přístupné 24 hodin denně, 7 dní v týdnu. Banka se však nezavazuje umožnit jejich využití bez přerušení a nepřetržitě. Banka je oprávněna přerušit nebo omezit poskytování Internetového bankovnictví na dobu nezbytnou k údržbě zařízení potřebných k jeho provozu. Banka si vyhrazuje právo zablokovat přístup ke službám Internetového bankovnictví nebo změnit či pozastavit poskytování služeb Internetového bankovnictví na dobu nezbytně nutnou, bude-li to zapotřebí z důležitých, zejména bezpečnostních nebo technických důvodů (zejm. při podezření na neoprávněné nebo podvodné použití Platebního prostředku, tedy např. při podezření na převzetí kontroly či snahu o převzetí kontroly nad Internetovým bankovnictvím neoprávněnou osobou, při podezření na infikování zařízení pro přístup do Internetového bankovnictví škodlivým malware, při zachycení signálu na root/jailbreak) nebo významného zvýšení rizika, že Klient nebude schopen splácet úvěr, který lze čerpat prostřednictvím daného Platebního prostředku); o zablokování Banka Uživatele zpraví předem a není-li to možné, pak následně s uvedením důvodů pro zablokování, ledaže k takovému oznámení není Banka dle právních předpisů povinna; oznámení může Banka provést zejména telefonicky, SMS zprávou či písemně. Pominou-li důvody pro zablokování Platebního prostředku, Banka Platební prostředek odblokuje nebo jej nahradí novým, tj. zejména vydá Uživateli nové personalizované bezpečnostní prvky; z bezpečnostních či technických důvodů je Banka oprávněna umožnit vydání nových personalizovaných bezpečnostních prvků pouze na Pobočce, pokud po individuální dohodě s Uživatelem nebude zvolen jiný způsob předání respektující bezpečnostní pravidla. Banka je oprávněna zablokovat přístup do Internetového bankovnictví jako celku, případně do některé z jeho aplikací, také v případě podezření na zneužití přístupu do Internetového bankovnictví, přičemž za takové podezření může Banka považovat i opakované neúspěšné pokusy o autentizaci z důvodu špatného zadání jakéhokoliv personalizovaného bezpečnostního prvku.

2.2.14 Banka není odpovědná za případy, kdy nelze využít služeb Internetového bankovnictví z důvodů mimo kontrolu Banky nebo jejích partnerů (například při přerušení dodávek elektrické energie, přerušení spojení s Bankou prostřednictvím veřejné sítě internet, poruchách na straně mobilního operátora, stávce apod.).

2.2.15 Sítě elektronické komunikace sloužící pro komunikaci mezi Bankou a Uživatelem dle těchto OP nejsou pod přímou kontrolou Banky a Banka tak neodpovídá za škodu způsobenou Uživateli či jinému Klientovi jejich případným zneužitím. Ochranu těchto sítí a důvěryhodnost jimi zasílaných zpráv jsou povinni zajišťovat příslušní poskytovatelé služeb elektronické komunikace (zejména ve smyslu zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů).

2.2.16 Banka zajišťuje chod služeb Internetového bankovnictví v souladu se Smlouvou o IB, včetně jejích nedílných součástí, zejména těchto OP a Sdělení. Banka předává Uživateli personalizované bezpečnostní prvky takovým způsobem, aby bylo možné tyto prvky použít jen oprávněným Uživatelem.

2.2.17 Uživatel je povinen využívat služby Internetového bankovnictví v souladu se Smlouvou o IB, Manuálem k IB a případnými dalšími pokyny Banky. Banka odpovídá za funkčnost služeb Internetového bankovnictví za předpokladu, že je uvedené Uživatelem dodržováno.

2.2.18 V rámci Internetového bankovnictvím může Uživatel podávat žádosti, zasílat Bance dokumenty a činit jiná právní jednání (zejména zadávat Platební příkazy), je-li mu to v rámci Internetového bankovnictví Bankou umožněno a upravují-li tak příslušné Smlouvy uzavřené s Bankou či Dispoziční oprávnění. Uvedená právní jednání Banka akceptuje za předpokladu, že budou učiněna Uživatelem, který je současně oprávněn tato právní jednání učinit dle podmínek příslušných Smluv či Dispozičních oprávnění. Právní jednání učiněná v Internetovém bankovnictví považujeme za učiněná v písemné formě.

2.2.19 V rámci Internetového bankovnictví může Uživatel uzavírat s Bankou i Smlouvy o některých dalších Finančních službách, tzv. Distančním způsobem (k tomu viz blíže VOP), je-li mu to v rámci Internetového bankovnictví Bankou umožněno. Způsob uzavření takové Smlouvy Banka určí s ohledem na konkrétní typ Smlouvy a technické možnosti Internetového bankovnictví.

2.2.20 V rámci příslušných aplikací Internetového bankovnictví mohou být Klientovi poskytovány Finanční služby spočívající v zaznamenávání a následné analýze příjmů a výdajů Klienta, přičemž Klientovi umožňují pracovat s daty získanými z jeho Platebních účtů, což zahrnuje širokou škálu funkčností pro práci s daty Klienta, zejména kategorizaci jednotlivých příjmů či výdajů, jejich třídění, vývojové grafy transakcí, zřizování virtuálních účtů pro správu transakcí, přiřazování fotografií, textů a jiného obsahu Klientem.

2.2.21 Prostřednictvím Internetového bankovnictví může být v závislosti na zaznamenaných datech i bez ohledu na ně poskytnuta rada či doporučení v oblasti financí Klienta, případně obchodní nabídka či sdělení. Klient bere na vědomí a souhlasí s tím, že taková rada, doporučení či nabídka nejsou právním poradenstvím, investičním poradenstvím ani jakoukoliv jinou profesionální radou a Banka za ně nepřebírá žádné záruky. Je vždy na výlučném rozhodnutí Klienta jak s takovou radou, doporučením či nabídkou naloží, případně zda na základě nich provede své osobní rozhodnutí, přičemž Banka neodpovídá za jakoukoliv škodu způsobenou Klientovi nebo třetí osobě v souvislosti s využitím takové rady, doporučení či obchodní nabídky.

2.2.22 Uživatel je povinen průběžně kontrolovat, zda zprávy o provedení požadavků učiněných prostřednictvím služeb Internetového bankovnictví odpovídají zadání Uživatele a zda byly zadané požadavky Uživatele Bankou provedeny nebo odmítnuty.

Uživatel je povinen zjištěné nesrovnalosti a závady v provedení neprodleně reklamovat v souladu s Reklamačním řádem Banky.

2.2.23 Banka odpovídá pouze za Bankou přijatá a potvrzená data. Banka neodpovídá za případné škody vzniklé chybným nebo duplicitním zadáním dat (požadavků k provedení Platební transakce).

2.2.24 Veškeré informace o systému Internetového bankovnictví a službách Internetového bankovnictví a jejich využití mají důvěrný charakter a Uživatel se zavazuje tyto nepoužít v rozporu s účelem, ke kterému byly poskytnuty.

2.2.25 Banka má oprávnění změnit vzhled a formát Internetového bankovnictví bez předchozího oznámení.

3 SLUŽBY NEPŘÍMÉ DÁNÍ PLATEBNÍHO PŘÍKAZU A INFORMOVÁNÍ O PLATEBNÍM ÚČTU

3.1.1 Banka Uživateli v rámci Internetového bankovnictví dále umožňuje:

a) využívání služby Nepřímého dání platebního příkazu a/nebo Informování o platebním účtu, poskytované třetí stranou – oprávněným poskytovatelem těchto služeb, k Platebnímu účtu Klienta vedeného u Banky;

b) poskytování služeb Nepřímého dání platebního příkazu a/nebo Informování o platebním účtu Bankou jako oprávněným poskytovatelem, k Platebním účtům Klienta vedeným u třetích stran, které umožňují poskytnutí těchto služeb.

3.1.2 Nepřímé dání platebního příkazu a/nebo Informování o platebním účtu je k dispozici pouze pro Platební účty, které mohou být obsluhovány prostřednictvím Internetového bankovnictví, respektive jsou přístupné prostřednictvím internetu. Prostředky komunikace mezi stranami a technické požadavky na vybavení Uživatele jsou totožné jako u využívání Internetového bankovnictví.

3.1.3 K využití Nepřímého dání platebního příkazu a/nebo Informování o platebním účtu prostřednictvím třetí strany musí Uživatel udělit souhlas v rámci rozhraní mezi Bankou a příslušným poskytovatelem dané služby, respektive mezi Bankou jako poskytovatelem dané služby a třetí stranou, která vede Klientovi Platební účet.

3.1.4 Dojde-li z jakéhokoli důvodu k ukončení závazků ze Smlouvy o IB uzavřené mezi Bankou a Klientem, Banka automaticky zruší možnost využívání služby Nepřímého dání platebního příkazu a/nebo Informování o platebním účtu, a to současně s ukončením přístupu do aplikací Internetového bankovnictví.

3.2 Služby poskytované třetí stranou – oprávněným poskytovatelem

3.2.1 Poskytování služeb Nepřímého dání platebního příkazu a/nebo Informování o platebním účtu Banka umožní pouze třetí straně, která je oprávněným poskytovatelem těchto platebních služeb podle zákona o platebním styku.

3.2.2 K propojení bankovního systému Banky s aplikací provozovanou třetí stranou slouží online rozhraní Banky. K získání přístupu k Platebnímu účtu prostřednictvím tohoto rozhraní je nutné vygenerování bezpečnostního klíče. K vygenerování bezpečnostního klíče dojde primárně automaticky pomocí aplikace třetí strany, která provede přesměrování do prostředí Banky, kde Uživatel udělí souhlas s napojením aplikace třetí strany pomocí zadání přihlašovacích personalizovaných bezpečnostních prvků do příslušné aplikace, pokud není ve vztahu k třetí straně uplatňován jiný způsob získání přístupu. Podrobný postup a způsob propojení (přístupu) je popsán v příslušném Manuálu k IB, který Banka zpřístupňuje na svých Internetových stránkách.

3.2.3 Pro Platební příkazy zadané nepřímo prostřednictvím oprávněné třetí strany dále platí náležitosti jako pro Platební příkazy podané prostřednictvím Internetového bankovnictví uvedené ve Sdělení.

3.2.4 Na Nepřímé dání platebního příkazu prostřednictvím třetí strany se vztahují limity pro Internetové bankovnictví a takto zadaný Platební příkaz je pro účely limitů považován za příkaz daný prostřednictvím Internetového bankovnictví.

3.2.5 Při využití služby Nepřímého dání platebního příkazu předá Banka oprávněnému poskytovateli této služby rovněž informaci ve smyslu čl. 2.9.3 VOP.

3.2.6 Prostřednictvím služby Informování o platebním účtu poskytované Uživateli třetí stranou, na základě souhlasu Uživatele poskytnutého Bance, Banka předá informace o Platebním účtu v rozsahu určeném Uživatelem, maximálně však ve stejném rozsahu, v jakém jsou přístupné Uživateli prostřednictvím služby Internetového bankovnictví.

3.2.7 Souhlas pro poskytování služby Informování o platebním účtu uděluje Uživatel při elektronické komunikaci mezi Bankou, Uživatelem a poskytovatelem služby Informování o platebním účtu. Souhlas je platný po dobu 180 dnů ode dne jeho udělení, přičemž po dobu platného souhlasu sděluje Banka Uživateli prostřednictvím poskytovatele informace o platebním účtu Klienta. Po uplynutí této doby musí Uživatel udělit tento souhlas opětovně, pokud není dále stanoveno jinak. Uživatel je oprávněn jej kdykoli odvolat.

3.2.8 Banka je oprávněna požadavek na sdělení informací poskytovateli služby Informování o platebním účtu odmítnout v případě, že:

a) má podezření na neoprávněné nebo podvodné použití Platebního prostředku nebo personalizovaných bezpečnostních prvků Klienta;

b) poskytovatel, který žádá o sdělení informací, není oprávněn poskytovat službu Informování o platebním účtu;

c) poskytovatel služby Informování o platebním účtu neosvědčil Bance svoji totožnost.

3.2.9 Informaci o odmítnutí sdělení informací Banka zpřístupní v rámci služby Internetového bankovnictví, případně sdělí Uživateli na jeho žádost.

3.3 Služby poskytované Bankou jako poskytovatelem

3.3.1 Banka je oprávněným poskytovatelem služeb Nepřímého dání platebního příkazu a/nebo Informování o platebním účtu podle zákona o platebním styku.

3.3.2 Banka poskytuje službu Nepřímého dání platebního příkazu a/nebo Informování o platebním účtu prostřednictvím aplikací CREDITAS Banking a CREDITAS Banking Mobile, kdy se příslušná aplikace se souhlasem Uživatele propojí se systémem provozovaným třetí stranou. Banka poskytuje Klientovi tyto služby pouze pro propojení s ověřenými třetími stranami, jejichž seznam průběžně aktualizuje.

3.3.3 Pro Nepřímé dání platebního příkazu a Informování o platebním účtu se kromě ustanovení tohoto článku 3 dále uplatní příslušná ustanovení Sdělení a VOP, kterými Banka plní svou informační povinnost vztahující se k poskytování těchto služeb.

4 BANKOVNÍ IDENTITA

4.1.1 Banka zřídí Uživateli, který:

a) dovršil věku 18 let,

b) alespoň jednou prokázal Bance svou totožnost osobně na Pobočce typem identifikačního dokladu, který může být ověřen v registru obyvatel,

c) jeho totožnost byla Bankou úspěšně ověřena v NIA; Uživateli byl ze strany NIA přidělen bezvýznamový směrový identifikátor (dále jen **„BSI**“), který byl Bance zaslán, je Bankou evidován a ve vztahu k Uživateli využíván v rámci komunikace mezi Bankou a NIA; došlo ze strany Banky k zápisu Uživatelova prostředku pro elektronickou identifikaci, jak je popsán v bodě 4.1.2 níže, u NIA,

d) má unikátní Registrované ČMT, tj. Banka Registrované ČMT tohoto Uživatele neeviduje zároveň jako Registrované ČMT jiného Uživatele,

automaticky službu Bankovní identita, pokud Uživatel před jejím zřízením Bance prokazatelně nesdělí, že zřízení této služby odmítá.

4.1.2 Využití služby Bankovní identity je možné prostřednictvím přihlašovacího jména a bezpečnostních prvků Uživatele používaných v kombinaci pro přístup do Internetového bankovnictví, jak jsou popsány v rámci Silného ověření v těchto OP, které se po úspěšném ověření Uživatele v NIA stanou tzv. prostředkem pro elektronickou identifikaci Uživatele evidovaným v Bance a zapsaným v evidenci vydaných prostředků pro elektronickou identifikaci u NIA (dále jen „**prostředek pro elektronickou identifikaci**“).

4.1.3 Jakmile bude Uživateli služba Bankovní identity zřízena, je Uživatel povinen bezodkladně prostřednictvím Internetového bankovnictví ověřit, že jsou jeho údaje zobrazované Bankou v Internetovém bankovnictví, resp. prostředku pro elektronickou identifikaci správně a jsou aktuální; Uživatel je povinen nesprávné či neaktuální údaje neprodleně oznámit Bance, případně, umožňuje-li to Banka, tyto údaje aktualizovat přímo v Internetovém bankovnictví.

4.1.4 Službu Bankovní identity, resp. platnost prostředku pro elektronickou identifikaci, může Uživatel prostřednictvím Internetového bankovnictví zřídit, pozastavit, zrušit nebo znovu aktivovat. Uvedené může Uživatel provést rovněž osobně na Pobočce. Pozastavení a zrušení je možné provést i telefonicky prostřednictvím infolinky Banky.

4.1.5 Banka je oprávněna zablokovat službu Bankovní identity, ať už dočasně či trvale, ve stejných případech, jako je dle těchto OP oprávněna zablokovat přístup do Internetového bankovnictví nebo na základě ohlášení Uživatele o zneužití nebo hrozícím zneužití prostředku pro elektronickou identifikaci nebo v případě zneplatnění BSI ze strany NIA.

4.1.6 Okamžikem zrušení Internetového bankovnictví zaniká poskytování služby Bankovní identity.

4.1.7 Uživatel je povinen prostředek pro elektronickou identifikaci chránit stejným způsobem, jako své personalizované bezpečnostní prvky používané pro přístup do Internetového bankovnictví dle těchto OP (viz Silné ověření), a to s náležitou péčí tak, aby minimalizoval možnost jeho zneužití. Uživatel je dále povinen se seznámit s Manuálem k IB, zejména dokumentem Informace k používání Internetového bankovnictví a Bankovní identity dostupným na Internetových stránkách a dodržovat zásady bezpečnosti v něm uvedené. V případě porušení povinnosti chránit prostředek pro elektronickou identifikaci se uplatní důsledky stanovené níže v bodě 5.1.5 stejně. Uživatel je také povinen bez zbytečného odkladu ohlásit Bance zneužití nebo hrozící nebezpečí zneužití prostředku pro elektronickou identifikaci, např. telefonicky prostřednictvím infolinky Banky.

4.1.8 Banka si vyhrazuje právo umožnit využití služby Bankovní identity pouze pro určitý typ služeb, a to zejména vůči soukromým poskytovatelům služeb, a rozsah poskytovaných služeb kdykoli měnit; rozsah poskytovaných služeb je uveden na Internetových stránkách. Banka si dále vyhrazuje právo poskytování služby Bankovní identita kdykoli ukončit, přičemž o této skutečnosti bude Uživatel informován v přiměřeném předstihu nebo nebude-li to možné bezprostředně poté.

5 PRAVIDLA BEZPEČNÉHO VYUŽÍVÁNÍ SLUŽEB A POVINNOSTI UŽIVATELE

5.1.1 Banka provádí ve své sféře vlivu preventivní opatření omezující riziko zneužití důvěrných informací v rámci Internetového bankovnictví a poskytování služeb Nepřímého dání platebního příkazu a Informování o platebním účtu.

5.1.2 Ustanovení tohoto článku shrnují základní pravidla bezpečného využívání služeb Internetového bankovnictví, Nepřímého dání platebního příkazu a Informování o platebním účtu.

5.1.3 Uživatel je povinen chránit personalizované bezpečnostní prvky služeb Internetového bankovnictví (zejména přihlašovací heslo, přihlašovací SMS kód, autorizační SMS kód, MPIN a biometrické údaje) před jejich ztrátou, odcizením nebo zneužitím.

5.1.4 Uživatel je povinen na své náklady provést taková opatření za účelem zajištění bezpečnosti personalizovaných bezpečnostních prvků Internetového bankovnictví a dalších důvěrných informací v rámci Internetového bankovnictví, která jsou s ohledem na obvyklá rizika porušení ochrany důvěrných informací technicky možná a přiměřená, a dále také zajistit bezpečnost zařízení pro využití Internetového bankovnictví a telefonu s Registrovaným ČMT, a proto se Uživatel zavazuje dodržovat zejména níže uvedená preventivní a bezpečnostní opatření a postupy k zajištění bezpečnosti důvěrných informací:

a) nezaznamenávat si personalizované bezpečnostní prvky Internetového bankovnictví, neukládat je na žádné trvalé nosiče dat, případně je uschovat jednotlivě od sebe mimo dosah jiných osob, resp. nezaznamenávat je tak, aby se dalya spojit s příslušnou Finanční službou;

b) nezadávat personalizované bezpečnostní prvky Internetového bankovnictví před jinou osobou, nesdělovat personalizované bezpečnostní prvky Internetového bankovnictví jiným osobám, a to ani rodinným příslušníkům a osobám blízkým; dále neumožnit automatické zapamatování personalizovaných bezpečnostní prvků Internetového bankovnictví pro přístup do Internetového bankovnictví, obzvláště pokud komunikační zařízení využívá více osob;

c) stanovit volitelné personalizované bezpečnostní prvky Internetového bankovnictví dle pravidel stanovených v Manuálu k IB, zejména bez zřejmé vazby ke své osobě nebo jeho osobám blízkým a pravidelně je aktualizovat; přístupové heslo/kód má být silné, jedinečné (tedy nepoužívané pro přístup k jiným službám), neodvoditelné a neodhadnutelné (tedy žádná jména rodinných příslušníků, zvířecích mazlíčků, adres, rodných čísel, dat narození atp.), ideálně je kombinací velkých a malých písmen, čísel a speciálních znaků;

d) měnit volitelné personalizované bezpečnostní prvky Internetového bankovnictví výhradně na Pobočkách Banky anebo prostřednictvím Internetového bankovnictví, nebo jiným bezpečným způsobem předem dohodnutým s Bankou; změnit si volitelné personalizované bezpečnostní prvky Internetového bankovnictví okamžitě při podezření na jejich vyzrazení;

e) nezasílat personalizované bezpečnostní prvky Internetového bankovnictví nebo osobní údaje Uživatele na jakoukoli výzvu zaslanou formou e-mailu, SMS nebo prostřednictvím sociálních sítí a komunikačních aplikací, dále ani ústně nesdělovat třetí osobě (a to ani pracovníkům Banky) své personalizované bezpečnostní prvky, a každou takovou výzvu dle tohoto odstavce bez zbytečného odkladu oznámit Bance; Banka nikdy takové údaje v elektronické komunikaci s Uživatelem nepožaduje a personalizované bezpečnostní prvky v ústní komunikaci pro ověření totožnosti Uživatele nevyužívá; v případě, kdy si Uživatel není jist, zda komunikuje s Bankou, nebo zda je komunikací ohrožena ochrana personalizovaných bezpečnostních prvků či zda hrozí zneužití Platebního prostředku, nesmí až do ujištění v komunikaci pokračovat a provádět žádné další úkony směřující k prolomení bezpečnosti těchto prvků a zpřístupnění Internetového bankovnictví třetí osobě, a musí ihned danou situaci konzultovat s Bankou;

f) zadávat personalizované bezpečnostní prvky služeb Internetového bankovnictví vždy jen do přihlašovacího formuláře na webových stránkách Banky https://banking.creditas.cz (přístup na tuto stránku je možný také skrze https://www.creditas.cz/), v důvěryhodném prohlížeči nebo při přihlašování do CBM, tedy v oficiální aplikaci Banky (tedy ani nepoužívat k přístupu do Internetového bankovnictví odkazů otevíraných ze sociálních sítí, e-mailů, SMS, aplikací pro vzájemnou komunikaci, internetových vyhledávačů, ani proklikem přes zobrazené sponzorované odkazy; přihlašovací formulář do Internetového bankovnictví umístěn na jiném webu nesmí být využit); v případě ověřování přes Bankovní identitu musí Uživatel zkontrolovat, že jsou přihlašovací údaje zadávány na webové stránce https://api.creditas.cz/oam/nia-saml-request-process; v souvislosti s uvedeným je také potřeba a sledovat, zda prohlížeč před zadáním personalizovaných bezpečnostních prvků Internetového bankovnictví nehlásí bezpečnostní varování, např. ohledně důvěryhodnosti certifikátu SSL serveru; v případě mobilních aplikací využívat pouze oficiální aplikace Banky stažené pouze z oficiálních úložišť (Google Play, App Store a Huawei App Gallery), Uživatel je oprávněn zadat personalizované bezpečnostní prvky za dodržení veškerých bezpečnostních opatření rovněž poskytovateli služby Nepřímého dání platebního příkazu nebo služby Informování o platebním účtu; Uživatel je však povinen dbát na to, aby tyto prvky zadával pouze takovým poskytovatelům, kteří jsou oprávněni danou službu poskytovat a jsou důvěryhodní (ověření těchto skutečností provádí na svoji odpovědnost Uživatel), stejně tak by Uživatel měl navštěvovat pouze důvěryhodné a známé internetové stránky a neotevírat podezřelé e-mailové přílohy (tj. s podezřelým předmětem, odesílatelem či textem), doporučováno je také v rámci e-mailové schránky využít filtr spamu; žádné jednání Banky nesmí být vykládáno jako ne/doporučení k poskytnutí personalizovaných bezpečnostních prvků konkrétnímu poskytovateli;

g) používat Internetové bankovnictví jen na zařízeních a v sítích, které jsou důvěryhodné a řádně zabezpečené proti zneužití

důvěrných informací; Uživatel nesmí používat Internetové bankovnictví zejména na veřejně přístupných zařízeních, např. v internetových kavárnách ~~a na jiných veřejně přístupných zařízeních~~, ani na zařízeních, u kterých nemá dostatečnou míru jistoty, že jsou zabezpečeny proti zneužití důvěrných informací; pro připojování do Internetového bankovnictví Uživatel nesmí využívat nezabezpečenou, veřejně přístupnou síť (např. nezabezpečenou wifi síť v ubytovacích zařízeních, restauracích, veřejných prostranstvích);

~~g)~~h) bezprostředně po ukončení práce s Internetovým bankovnictvím se z něj odhlásit, po ukončení práce s CREDITAS Banking Mobile tuto aplikaci zavřít a nenechávat ji otevřenou na pozadí v daném zařízení, před odhlášením z Internetového bankovnictví nebo zavřením CBM neponechávat dané zařízení bez dohledu;

~~h)~~i) legálně zabezpečit zařízení pro využití Internetového bankovnictví (tedy i mobilní telefon) antivirovou a antispyware ochranou, jakož i firewallem, a tyto ochranné prvky pravidelně aktualizovat, stejně jako operační systém daného zařízení; Uživatel má dále povinnost aktualizovat programy standardním způsobem a pravidelně sledovat informace o nových hrozbách, virech, spyware, malware apod. (např. informace v rámci bezpečnostních oznámení a upozornění zveřejněných Bankou na jejích Internetových stránkách, zejm. v aktualitách či na stránce https://www.creditas.cz/bezpecnost, dále zasílaných Bankou formou e-mailů či zpráv v rámci Internetového bankovnictví, ale i z jiných zdrojů), informovat se o aktuálních možnostech zabezpečení daného zařízení, a v souladu s tím zajistit ochranu takového zařízení;

~~i)~~j) na zařízení pro využití Internetového bankovnictví nestahovat a neinstalovat volně dostupné programy, u nichž si nemůže být jist, že neobsahují viry, malware nebo spyware, zejména programy, které nepocházejí z důvěryhodných zdrojů, a zařízení zabezpečit před vzdáleným přístupem jiných osob zejm. tím, že nepovolí instalaci software umožňujícího vzdálené připojení k zařízení; dále využívat pouze oficiální verzi CBM staženou pouze z oficiálních úložišť a zdrojů pro příslušný operační systém daného zařízení (Google Play, App Store a Huawei App Gallery); stejná opatření by měl Uživatel dodržet i v případě jiných mobilních aplikací, přičemž by se však Uživatel u stahovaných aplikací neměl spolehnout pouze na kontrolu bezpečnosti prováděnou ze strany provozovatele daného uložiště – Uživatel by měl mít na paměti, že bezpečná aplikace stažená z oficiálního zdroje může následně vyžadovat aktualizaci, která může obsahovat škodlivý malware; Uživatel dále odpovídá za rozsah oprávnění, který udělí příslušné aplikaci (tedy měl by aplikaci umožnit jen takový přístup k údajům a obsahu, který je v daném rozsahu a času užívání skutečně nezbytný pro fungování dané aplikace, zároveň by měl zvážit, zda aplikace, která si vynucuje přístup k údajům a oprávnění nad rámec logiky svého fungování, je vhodná k instalaci do zařízení pro využití Internetového bankovnictví či do telefonu s Registrovaným ČMT);

~~j)~~k) v případě nedostatečné znalosti nastavení zabezpečení zařízení pro využití Internetového bankovnictví kontaktovat Banku, resp. ~~nebo~~ se přímo obrátit na odborníka v oblasti kybernetické bezpečnosti;

~~k)~~l) telefon s Registrovaným ČMT pro zasílání SMS kódů souvisejících s Internetovým bankovnictvím technologicky chránit obdobně jako zařízení pro využití služeb Internetového bankovnictví (tedy prostřednictvím antivirové a antispyware ochrany, jakož i firewallem, případně jiným aktuálním způsobem zabezpečení) a tyto ochranné prvky pravidelně aktualizovat a zabezpečit tento telefon nejen před vzdáleným přístupem jiných osob;

~~l)~~m) mít ~~telefon~~ zařízení využíván~~ý~~é v souvislosti s Internetovým bankovnictvím stále pod kontrolou a nepůjčovat jej (či jeho SIM kartu) jiným osobám bez dostatečného dohledu nad jejich nakládáním s tímto ~~telefonem~~zařízením;

~~m)~~n) zabezpečit ~~telefon~~ zařízení využíván~~ý~~é v souvislosti s Internetovým bankovnictvím biometrickým zabezpečením přístupu do zařízení, případně ~~-~~přístupovým kódem (číselným či grafickým) pro znemožnění užití ~~telefonu~~ zařízení jinou osobou, který je silný, jedinečný, neodvoditelný a neodhadnutelný.; a takový přístupový kód uchovávat v tajnosti a nesdělovat ho jiným osobám, ani ho nikam nezaznamenávat;

o) nevyužívat pro přístup do Internetového bankovnictví ~~telefony~~zařízení, u kterých byly provedeny úpravy označované jako root nebo jailbreak nebo jiné zásahy do software ~~telefonu~~zařízení;

p) v případě, kdy je zařízení sloužící k přístupu do Internetového bankovnictví či telefon s Registrovaným ČMT napaden škodlivým malwarem (ten může např. umožnit třetí osobě vzdáleně ovládat Internetové bankovnictví, vytěžit SMS s autorizačním kódem a přeposlat jej třetí osobě a/nebo může umožnit zpřístupnění citlivých uživatelských dat a bezpečnostních prvků třetím osobám), případně bylo detekováno riziko působení škodlivého malwaru v daném zařízení, je Uživatel povinen infikované zařízení vyčistit – jelikož malware nemusí napadat jen aplikaci CREDITAS Banking Mobile, ale i jiné aplikace (nejen bankovní), je žádoucí v uvedeném případě vyčistit zařízení i pro ochranu Uživatele obecně – malware často nelze odstranit pouhou odinstalací aplikací nebo obnovením zařízení do továrního nastavení, je proto vhodné obrátit se na odbornou pomoc (kvalifikovaný servis či odborníka v oblasti kybernetické bezpečnosti); v případě, kdy je ze strany Banky detekována přítomnost malwaru na zařízení Uživatele, a tedy ohrožena bezpečnost Platebního prostředku, je Banka oprávněna zablokovat přístup Uživatele ke službám Internetového bankovnictví, a to v případě potřeby i opakovaně;

q) pozorně číst oznámení zaslaná Bankou v SMS, e-mailu, push notifikaci atp. – zejména musí Uživatel věnovat pozornost nevyžádaným oznámením o jednáních, která Uživatel neinicioval, např. o aktivaci CBM na novém zařízení, o přihlášení do Internetového bankovnictví, změně kontaktního e-mailu či o aktivaci digitální peněženky, a bezodkladně o tom informovat

Banku; Bankou zaslané potvrzovací kódy nepředávat žádné třetí osobě ani nenechávat zařízení s přijatým potvrzovacím kódem bez dozoru a přístupné třetí osobě;

~~n)~~r) u přijatých platebních instrukcí před realizací platby vždy zkontrolovat výši částky, název obchodníka a účet příjemce; při nákupu v neznámých e-shopech a u neznámých obchodníků předem vyhledat důvěryhodné reference a zkontrolovat si obsah internetových stránek obchodníka (např. zda fungují veškeré prokliky, zda jsou vyplněny kontaktní údaje obchodníka a jiné informace, zda obchodník plní povinnost uvádět obchodní podmínky a zda je v nich relevantní text) – pokud stránky působí nedokončeným dojmem nebo jsou na nich zobrazeny neúplné informace, může jít o podvodné stránky a Uživatel by jejich prostřednictvím neměl nakupovat;

s) okamžitě telefonicky (přednostně na nonstop infolince **+420 583 037 088**) ~~nebo elektronicky~~, případně osobně na Pobočce Banky či elektronicky, informovat Banku v případě podezření na jakoukoli programovou chybu systému Internetového bankovnictví nebo chybu, ztrátu, odcizení či zneužití Platebního prostředku či ve vztahu k personalizovaným bezpečnostním prvkům Internetového bankovnictví (např. zničení, ztráta nebo odcizení zařízení pro využití Internetového bankovnictví anebo telefonu využívaného v souvislosti s Internetovým bankovnictvím či jejich napadení viry) anebo k zasílání nebo přijímání Platebních transakcí a následně s Bankou účinně spolupracovat při realizaci jí navržených nápravných opatření; Banka je po každém takovém oznámení oprávněna zrušit možnost využívání Internetového bankovnictví; pro vyloučení všech pochybností se sjednává, že obdobné informační a kooperační povinnosti má Uživatel i ve vztahu k Nepřímému dání platebního příkazu či Informování o platebním účtu, jakož i při podezření týkajícího se poskytovatelů těchto služeb; pro lepší kontrolu nad případným neoprávněným užíváním Platebního prostředku Banka doporučuje nastavit ze strany Uživatele notifikace informující o pohybech na účtu a také bezpečnostní limity pro online převody.

5.1.5 **Nedodržení opatření a postupů** uvedených v předchozím bodě těchto OP může vést k zneužití důvěrných informací či personalizovaných bezpečnostních prvků Internetového bankovnictví a ke vzniku újmy Uživateli nebo jinému Klientovi či třetí osobě. Nedodržení těchto opatření a pravidel je Banka oprávněna považovat za **hrubou nedbalost, resp. podstatné porušení Smlouvy o IB**. V důsledku této nedbalosti Uživatel odpovídá v plné výši za veškeré újmy způsobené jemu, nebo jinému Klientovi či třetí osobě do okamžiku nahlášení ztráty, odcizení či zneužití personalizovaných bezpečnostních prvků Internetového bankovnictví nebo dalších důvěrných informací v rámci Internetového bankovnictví Bance.

5.1.6 V případě, že Bance vznikne podezření na neoprávněné nebo podvodné použití ~~p~~Platebního prostředku informuje o tomto Banka Klienta způsobem uvedeným ve VOP.

6 ROZSAH FINANČNÍCH SLUŽEB A SAZEBNÍK POPLATKŮ

6.1.1 Rozsah základních Finančních služeb poskytovaných Bankou v rámci Internetového bankovnictví vyplývá z ustanovení bodu 2.2.18, 2.2.19, 2.2.20 a 3.3 těchto OP.

6.1.2 Úplata za Finanční služby poskytované v rámci Internetového bankovnictví, ostatní Finanční služby poskytované v rámci Internetového bankovnictví, úplata za ně, případně sankce související s Internetovým bankovnictvím jsou uvedeny v příslušném Sazebníku Banky.

6.1.3 Úplata za Finanční služby poskytované v rámci Internetového bankovnictví, ostatní Finanční služby poskytované v rámci Internetového bankovnictví, úplata za ně, případně sankce související s Internetovým bankovnictvím jsou pro Klienty mladší 18 let uvedeny v příslušném Sazebníku Banky pro Richee produkty Junior. Dovršením věku 18 let Klienta se pro Internetové bankovnictví uplatní příslušný aktuální Sazebník Banky pro fyzické osoby nepodnikající.

7 ZÁVĚREČNÁ USTANOVENÍ

7.1 Zrušovací ustanovení

7.1.1 Tyto OP pro Internetové bankovnictví v den nabytí své účinnosti ruší a nahrazují OP účinné od ~~27. 7. 2023~~8. 1. 2024.

7.2 Přechodná ustanovení

7.2.1 Neuplatní se.

7.3 Účinnost

7.3.1 Tyto OP nabývají účinnosti dne ~~8. 1. 2024~~ 1. 10. 2024.