OBCHODNÍ PODMÍNKY BANKY CREDITAS A.S. PRO VYUŽÍVÁNÍ SLUŽEB INTERNETOVÉHO BANKOVNICTVÍ – DIVIZE MAX

ÚČINNÉ OD 15. 11. 2025

OBSAH

1. PŘEDMĚT ÚPRAVY A ROZSAH POUŽITÍ 2
2. DEFINICE 2
3. PŘEDPOKLADY PRO POUŽÍVÁNÍ INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ 3
4. DORUČOVÁNÍ A KOMUNIKACE PROSTŘEDNICTVÍM INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ 3
5. PŘÍSTUP DO INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ 3
6. PŘIJÍMÁNÍ PŘÍKAZŮ V RÁMCI PLATEBNÍCH SLUŽEB 4
7. NEOBVYKLÉ UDÁLOSTI, PORUCHY INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ, SERVISNÍ SLUŽBY 5
8. ODPOVĚDNOST KLIENTA 5
9. REKLAMACE 5
10. UKONČENÍ OBCHODNÍHO VZTAHU 5
11. PRAVIDLA BEZPEČNÉHO VYUŽÍVÁNÍ SLUŽEB A POVINNOSTI UŽIVATELE 6
12. ZÁVĚREČNÁ USTANOVENÍ 8

1. PŘEDMĚT ÚPRAVY A ROZSAH POUŽITÍ

1.1 Banka CREDITAS a.s. – Divize Max vydává ve smyslu svých Všeobecných obchodních podmínek Banky CREDITAS a.s. – Divize Max (dále jen „**VOP**“) a Podmínek pro provádění platebního styku Banky CREDITAS a.s. – Divize Max (dále jen „**Podmínky platebního styku**“) k úpravě vzájemných práv a povinností při užívání systému Internetového bankovnictví tyto Obchodní podmínky Banky CREDITAS a.s. pro používání služeb Internetového bankovnictví – Divize Max (dále jen „**Speciální podmínky**“).

1.2 Speciální podmínky jsou doplněním, Podmínek platebního styku a VOP a součástí individuálních smluv mezi Klientem a Bankou o poskytnutí přístupu k Internetovému bankovnictví, kdykoliv na ně taková individuální smlouva odkazuje.

1.3 V případě rozporu mezi ustanoveními individuální smlouvy a ustanoveními těchto Speciálních podmínek, Podmínek platebního styku nebo VOP mají ustanovení individuální smlouvy přednost. Záležitosti, které nejsou upraveny individuální smlouvou, se řídí těmito Speciálními podmínkami, nebo Podmínkami platebního styku, nebo VOP podle uvedeného pořadí.

2. DEFINICE

Pojmy používané v těchto Speciálních podmínkách a uváděné s velkými počátečními písmeny mají význam definovaný níže nebo výše v textu těchto Speciálních podmínek nebo ve VOP:

Autorizační telefonní číslo – unikátní mobilní telefonní číslo s českou nebo slovenskou předvolbou, které má Uživatel sjednané s Bankou pro účely využívání služeb Internetového bankovnictví. Uživatel může mít pouze jedno Autorizační telefonní číslo. Změnu Autorizačního telefonního čísla může Uživatel provést prostřednictvím Internetového nebo Mobilního bankovnictví, případně na základě žádosti podané osobně (případně prostřednictvím zmocněné osoby) na Provozovně Banky nebo zaslané prostřednictvím pošty na Provozovnu Banky, pokud je podpis Uživatele na této žádosti úředně ověřen;

Banka – Banka CREDITAS a.s., se sídlem Sokolovská 675/9, Karlín, 186 00 Praha 8, IČO: 63492555, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 23903;

Bankovní data – data v elektronické podobě určená pro přenos, jejichž výměna je předmětem poskytovaných služeb;

Bezpečnostní kód – kód, zaslaný Bankou Uživateli SMS zprávou na Autorizační telefonní číslo, sloužící pro přístup Uživatele do Internetového bankovnictví a pro autorizaci platebních příkazů a operací prováděných Uživatelem v rámci Internetového bankovnictví;

Biometrický údaj – osobní údaj technického charakteru zpracování fyzických či fyziologických znaků fyzické osoby, který umožňuje jedinečnou identifikaci Klienta;

Heslo – řetězec písmen, číslic a znaků umožňující přístup do Internetového bankovnictví;

Informování o platebním účtu – 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;

Internetové bankovnictví – pro účely těchto podmínek se internetovým bankovnictvím míní Internetové bankovnictví banky dostupné na ib.maxbanka.eu;

Internetové stránky Banky – jsou k dispozici na adrese (URL) www.maxbanka.eu;

Kontaktní centrum – kontaktní centrum Banky, poskytující přístup k vybraným službám Banky prostřednictvím prostředků vzdálené komunikace, dostupné na kontaktních údajích zveřejněných na Internetové stránce Banky;

Mobilní aplikace – aplikace určená pro ovládání účtů vedených Bankou – Divize Max, přihlašování, autorizaci platebních příkazů a požadavků v Internetovém bankovnictví prostřednictvím mobilních zařízení;

Mobilní bankovnictví – Internetové bankovnictví ovládané prostřednictvím Mobilní aplikace;

MPIN – osobní identifikační kód Uživatele, sloužící k ověření totožnosti osoby zadávající tento kód;

Nepřímé dání platebního příkazu – 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;

Notifikace – vyžádané SMS, e-mailové zprávy nebo push notifikace, kterými Banka informuje Klienta o událostech spojených s využíváním služeb;

Oprávněný uživatel – fyzická osoba, které byla na základě žádosti Klienta a v jím určeném rozsahu udělena Přístupová oprávnění k účtu/účtům a dalším produktům Klienta prostřednictvím Internetového nebo Mobilního bankovnictví;

Příkaz – příkaz nebo žádost zadaná Uživatelem Bance prostřednictvím Internetového nebo Mobilního bankovnictví;

Přístupová oprávnění – soubor autorizačních oprávnění, vymezující účty a jiné služby, s nimiž bude disponováno a jež budou užívány prostřednictvím Internetového nebo Mobilního bankovnictví, a osoby oprávněné k dispozici s těmito účty a jinými službami, včetně určení rozsahu a způsobu těchto dispozičních oprávnění;

Smlouva – Smlouva o používání služeb Internetového bankovnictví uzavřená mezi Bankou a Uživatelem, případně jiná smlouva v rozsahu platného ujednání o přístupu Uživatele do Internetového bankovnictví na základě takové smlouvy;

Třetí strana – subjekt licencovaný a oprávněný k poskytování služby Nepřímého dání platebního příkazu a/ nebo služby Informování o platebním účtu;

Uživatel – fyzická osoba, Klient nebo Oprávněný uživatel Internetového a Mobilního bankovnictví s definovanými Přístupovými oprávněními k účtům a produktům Klienta;
Uživatelské jméno – uživatelské jméno, pod kterým se Uživatel hlásí do Internetového bankovnictví;

3. PŘEDPOKLADY PRO POUŽÍVÁNÍ INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ

3.1 Technické požadavky pro *Internetové a Mobilní bankovnictví*:
Technické požadavky pro používání Internetového a Mobilního bankovnictví jsou dostupné na internetových stránkách Banky CREDITAS a.s. – Divize Max: www.maxbanka.eu. Uživatel se zavazuje se s technickými požadavky a opatřeními seznámit a řídit se jimi.

3.1.1 Hardware – klientská stanice pro Internetové bankovnictví musí splňovat požadavky minimální konfigurace stanovené poskytovateli jednotlivých webových prohlížečů.

3.1.2 Software – aktuální verze webových prohlížečů Google Chrome, Mozilla Firefox, Apple Safari nebo Microsoft Edge. Přístup ze zastaralých či nepodporovaných webových prohlížečů může být z bezpečnostních důvodů zablokován.

3.1.3 Pro přístup do Mobilního bankovnictví je potřeba mít na svém mobilním zařízení nainstalovanou Mobilní aplikaci, kterou lze stáhnout u poskytovatele aplikací dle operačního systému mobilního zařízení Uživatele. Mobilní aplikace je Bankou distribuována prostřednictvím oficiálních zdrojů Google Play a App Store. Klient je povinen neinstalovat Mobilní aplikaci z jiných než z těchto oficiálních zdrojů.

3.2 Podpisem Smlouvy Uživatel Bance zaručuje svou technickou připravenost k používání přístupu pro využívání služeb Internetového a Mobilního bankovnictví. Uživatel bere na vědomí, že pokud nemá k dispozici potřebný software a/nebo hardware, není Banka schopna garantovat bezchybné používání Internetového a Mobilního bankovnictví.

3.3 Banka si vyhrazuje právo změny technických požadavků pro Internetové a Mobilní bankovnictví tak, aby při případném zkvalitňování či rozšiřování služeb mohl Uživatel využívat Internetové a Mobilní bankovnictví stále v plném rozsahu.

4. DORUČOVÁNÍ A KOMUNIKACE PROSTŘEDNICTVÍM INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ

4.1 **Doručování dokumentů**
Banka se s Klientem dohodla, že dokumentaci (smlouvy, dodatky apod.) týkající se služeb a produktů může Banka doručovat do elektronického úložiště (archivu dokumentů) přístupném v Internetovém nebo Mobilním bankovnictví. Banka a Klient se dále dohodli, že Klient je oprávněn doručovat Bance dokumentaci (zejména žádosti) týkající se služeb a produktů, a to prostřednictvím Internetového nebo Mobilního bankovnictví. Banka a Klient se dále dohodli, že Banka je oprávněna jednostranně neakceptovat dokumenty doručené Klientem prostřednictvím Internetového nebo Mobilního bankovnictví, přičemž Banka tak může učinit bez udání důvodu. V případě, že Banka neakceptuje dokumenty, které jí zaslal Klient prostřednictvím Internetového nebo Mobilního bankovnictví, pak o takové skutečnosti Klienta vyrozumí. Banka se s Klientem dohodla, že dokumenty, které Klient zašle prostřednictvím Internetového nebo Mobilního bankovnictví Bance, budou ve formátu pdf.

4.2 **Vzájemná komunikace**
Banka se s Klientem dohodla, že vzájemná komunikace mezi Bankou a Klientem může probíhat také formou zpráv zasílaných prostřednictvím Internetového nebo Mobilního bankovnictví.

4.3 **Žádosti o produkty a uzavírání smluv**
Banka se s Klientem dohodla, že smlouvy, dodatky i další související dokumentace týkající se služeb a produktů Bankou nabízených, je možné uzavírat prostřednictvím Internetového nebo Mobilního bankovnictví, kde vlastnoruční podpis Klienta bude nahrazen elektronickým podpisem spočívajícím v zadání obdrženého Bezpečnostního kódu nebo MPINU pomocí elektronického úkonu učiněného Klientem v Internetovém nebo Mobilním bankovnictví. Takový způsob právního jednání bude Klientovi umožněn pouze v případech stanovených Bankou.

4.4 **Mobilní bankovnictví**
Mobilní bankovnictví umožňuje přihlašování, autorizaci platebních příkazů a požadavků a ovládání účtů vedených Bankou v rozsahu, v jakém to Mobilní aplikace umožní.

5. PŘÍSTUP DO INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ

5.1 Banka na základě Smlouvy umožní Uživateli prostřednictvím Internetového a Mobilního bankovnictví obsluhu těch finančních služeb, (i) které jsou vedeny na jméno tohoto Uživatele nebo pro něj, a to v rozsahu, ve kterém to Banka umožňuje, za předpokladu, že Uživatel si obsluhu příslušné finanční služby sám neomezil a (ii) které jsou vedeny na jméno jiného Klienta nebo pro tohoto Klienta, a to v rozsahu, ve kterém to Banka umožňuje, pokud k obsluze daných finančních služeb tento jiný Klient udělil Oprávněnému uživateli Přístupová oprávnění.

5.2 Smlouva mezi Uživatelem a Bankou může být uzavřena prostřednictvím Internetového bankovnictví, korespondenčně s úředně ověřeným podpisem nebo osobně po ověření pracovníkem Banky.

5.3. Přístupové oprávnění pro Oprávněné uživatele může Klient zřídit, změnit nebo odebrat prostřednictvím Internetového bankovnictví, korespondenčně s úředně ověřeným podpisem, případně osobně po ověření pracovníkem Banky.

5.4 Uživatel je oprávněn pracovat s Internetovým a Mobilním bankovnictvím dvacet čtyři (24) hodin denně. Banka je oprávněna omezit či přerušit provoz Internetového a Mobilního bankovnictví na dobu nezbytně nutnou pro jeho údržbu.

Přístup do Internetového bankovnictví:

5.5 Při přístupu do Internetového bankovnictví se za účelem autentizace Uživatele využívá dvoufaktorové ověření. Dvoufaktorové ověření spočívá ve využití kombinace dvou prvků z různých kategorií, kterými jsou „znalost“ (něco, co Uživatel zná, např. Heslo), „držení“ (něco, co Uživatel vlastní či má jinak ve svém oprávněném držení, např. mobilní telefon nebo jiné obdobné zařízení) a „inherence“ (něco, čím Uživatel je – sem patří Biometrické údaje, např. otisk prstu či snímek obličeje).

5.6 Internetové bankovnictví je Uživatelům přístupné prostřednictvím Internetových stránek Banky po provedení příslušné autentizace Uživatele ze strany Banky, tj. ověření a potvrzení totožnosti Uživatele Bankou, prostřednictvím zadání Uživatelského jména a následujících společných personalizovaných bezpečnostních prvků:

a) Hesla:

Heslo pro první přihlášení Uživatele obdrží Uživatel na samostatném dokumentu neprodleně po uzavření Smlouvy na Provozovně Banky nebo si jej Uživatel zvolí sám při uzavírání Smlouvy distančním způsobem; Uživatel je povinen si Heslo obdržené na samostatném dokumentu od Banky po prvním přihlášení do Internetového bankovnictví v jeho prostředí změnit;

b) Bezpečnostního kódu:

Bezpečnostní kód pro přihlášení je zasílán Uživateli po zadání přihlašovacího jména v rámci prostředí Internetových stránek Banky určeného pro přihlášení do Internetového bankovnictví.

V některých případech vyžaduje přihlášení do Internetového bankovnictví také za dání data narození. Namísto Bezpečnostního kódu a Hesla může být Uživatelem využita Mobilní aplikace instalovaná na mobilním zařízením Uživatele, která umožňuje Uživateli použít k přihlášení MPIN kód Mobilní aplikace (který si volí Uživatel) či Biometrický údaj Uživatele. Při další autentizaci Uživatele do Internetového bankovnictví může být kombinace Hesla a Bezpečnostního kódu nahrazena přihlášením prostřednictvím autentizace v Mobilní aplikaci po načtení přihlašovacího QR kódu.

5.7 Pro autorizaci platebního příkazu nebo jiného požadavku realizovatelného prostřednictvím Internetového bankovnictví Uživatel obdrží od Banky prostřednictvím SMS zprávy Bezpečnostní kód, jehož zadáním příslušný platební příkaz nebo jiný požadavek autorizuje. Namísto použití Bezpečnostního kódu může Uživatel autorizovat platební příkaz či jiný požadavek realizovatelný prostřednictvím Internetového bankovnictví zadáním MPIN kódu Mobilní aplikace (který si volí Uživatel) v Mobilní aplikaci instalované na mobilním zařízením Uživatele či prostřednictvím Biometrického údaje nastaveného tamtéž. U vybraných požadavků může Banka umožnit jejich autorizaci pouhým kliknutím na odpovídající potvrzovací tlačítko v Internetovém bankovnictví. Banka si vyhrazuje právo u vybraných požadavků umožnit pouze jí určený způsob autorizace.

5.8 Bezpečnostní kód je zasílán Uživateli na jeho riziko. Banka nenese odpovědnost za nedoručení Bezpečnostního kódu nebo doručení neplatného Bezpečnostního kódu v důsledku okolností mimo vliv Banky, zejména v případě chybného nebo přerušeného telekomunikačního spojení nebo v důsledku technické závady na přenosových zařízeních.

5.9 Uživatel může používat oba způsoby autorizace (Bezpečnostní kód a Mobilní aplikaci) souběžně. Podmínkou pro využívání Mobilní aplikace je její úspěšná registrace.

Přístup do Mobilního bankovnictví:

5.10 Do Mobilního bankovnictví se Uživatel přihlašuje zadáním MPIN nebo Biometrickým údajem. Pro registraci (aktivaci) Mobilní aplikace je podmínkou ověření identity Uživatele, a to prostřednictvím Uživatelského jména, data narození, Hesla a potvrzením Bezpečnostním kódem. V případě použití jednorázového hesla je po Uživateli v průběhu registrace vyžadováno nastavení nového hesla pro Internetové bankovnictví.

5.11 Autorizaci platebního příkazu nebo jiného požadavku realizovatelného prostřednictvím Mobilního bankovnictví Uživatel provádí zadáním MPIN kódu nebo Biometrickým údajem. U vybraných požadavků může Banka umožnit jejich autorizaci pouhým kliknutím na odpovídající potvrzovací tlačítko v Mobilním bankovnictví. Banka si vyhrazuje právo u vybraných požadavků umožnit pouze jí určený způsob autorizace.

6. PŘIJÍMÁNÍ PŘÍKAZŮ V RÁMCI PLATEBNÍCH SLUŽEB

6.1 Banka zpracovává zaslané Příkazy pouze do času uzávěrek. Časy uzávěrek jsou vyhlašovány Bankou a jsou k dispozici Klientovi na Kontaktním centru a případně též na Internetových stránkách Banky a v provozních prostorách Banky.

6.2 Pokud Banka obdrží Příkazy v den požadované splatnosti po času uzávěrky stanoveném pro daný typ transakce, je Banka oprávněna transakce zpracovat v nejbližším Bankovním pracovním dni.

6.3 Úmyslně vynecháno.

6.4 Banka odpovídá pouze za přijatá a potvrzená data, neodpovídá za přímé a nepřímé škody vzniklé chybným nebo duplicitním zasláním dat do Banky, za škody způsobené poruchou používané telekomunikační sítě, sítě internet, technickou poruchou na straně Klienta a za škody způsobené tzv. vyšší mocí (viz § 2913 odst. 2 Občanského zákoníku). Dále Banka neodpovídá za opoždění plateb dle zadaných zahraničních platebních příkazů, pokud je zpoždění zapříčiněno tím, že si Banka v souladu s případnými požadavky platných právních předpisů vyžádala předložení určitých dokladů (např. doklady prokazující účel platby nebo potvrzující splnění informačních povinností dle devizových předpisů). Pokud Klient doklady potřebné k provedení platby Bance nepředloží, nebude Banka povinna takovou platbu provést.

6.5 Pro operace prováděné prostřednictvím Internetového a Mobilního bankovnictví může Banka stanovit maximální denní limit pro převody peněžních prostředků. Tento limit může být stanoven po dohodě s Klientem nebo jednostranně Bankou. Banka

je oprávněna limit jednostranně změnit s ohledem na zákonná omezení nebo bezpečnostní politiku Banky. Případná změna výše limitu bude Klientovi s dostatečným časovým předstihem vhodným způsobem oznámena.

6.6 Provádění platebních Příkazů Klienta se v dalším řídí Zákonem o platebním styku a příslušnými ustanoveními Podmínek platebního styku a VOP.

6.7 Platební příkaz se autorizuje úspěšným zadáním Bezpečnostního kódu zaslaného prostřednictvím SMS nebo zadáním PIN kódu či použitím Biometrického údaje v Mobilní aplikaci. Platební příkaz Banka považuje za autorizovaný, pokud obsahuje nezbytný počet podpisů (autorizací) pro jeho zpracování.

7. NEOBVYKLÉ UDÁLOSTI, PORUCHY INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ, SERVISNÍ SLUŽBY

7.1 Uživatel je povinen bez zbytečného odkladu oznámit Bance jakoukoliv poruchu Internetového nebo Mobilního bankovnictví včetně jejího popisu.

7.2 V případě, že Uživatel pro vstup do Internetového bankovnictví použije opakovaně chybné přihlašovací údaje, nebo Bezpečnostní kód, dojde k automatickému dočasnému zablokování Uživatelova přístupu do Internetového bankovnictví.
V případě, že Uživatel při autorizaci opakovaně zadá chybný MPIN v Mobilní aplikaci, bude Mobilní aplikace automaticky odregistrována a je třeba provést opětovnou registraci.

7.3 Banka je oprávněna zablokovat přístup Uživatele do Internetového a Mobilního bankovnictví, pokud má podezření, že je ohrožena bezpečnost Klientova účtu nebo účtů. O zablokování přístupu a jeho důvodech bude v takovém případě Banka informovat Klienta bez zbytečného prodlení. Poskytování služby přístupu k Internetovému a Mobilnímu bankovnictví bude Uživateli obnoveno až poté, co pomine nebezpečí jeho zneužití, případně po přijetí nezbytných opatření. Uživatel je oprávněn požádat Banku o zablokování přístupu do Internetového nebo Mobilního bankovnictví. Zablokováním přístupu do Internetového nebo do Mobilního bankovnictví budou přerušeny služby Třetích stran.

7.4 Banka si vyhrazuje právo jednostranně bezplatně změnit Uživateli používaný typ přístupu do Internetového a Mobilního bankovnictví na přístup poskytující vyšší stupeň zabezpečení.

8. ODPOVĚDNOST KLIENTA

8.1 Úmyslně vynecháno

8.2 Klient bere na vědomí, že v případě přístupu do Internetového bankovnictví Heslo a Bezpečnostní kód a pro Mobilní aplikaci MPIN kód nebo Biometrický údaj slouží k ověření jeho totožnosti, resp. totožnosti Oprávněného uživatele pro přístup do Internetového bankovnictví.

8.3 Transakce a úkony autorizované Bezpečnostním kódem a pro Mobilní aplikaci MPIN kódem nebo Biometrickým údajem se považují za transakce uskutečněné Klientem, resp. Oprávněným uživatelem. Klient je plně odpovědný za veškeré transakce, které byly uskutečněny k tíži jeho účtu prostřednictvím dálkového přístupu a řádně ověřeny zadáním MPIN kódu, Bezpečnostního kódu nebo Biometrickým údajem.

8.4 Úmyslně vynecháno

8.5 Úmyslně vynecháno

8.6 Klient je povinen bezodkladně kontrolovat Bankou provedené operace, zda odpovídají jím zadaným Příkazům nebo Příkazům zadaným Oprávněným uživatelem. Zjištěné rozdíly je povinen okamžitě, nejdéle do 5 (pěti) Bankovních pracovních dnů od jejich zjištění, oznámit Bance písemnou formou. Pokud tak neučiní, spoluodpovídá za případně jemu vzniklou škodu.

8.7 Banka neodpovídá za škodu vzniklou v důsledku porušení podmínek příslušné Smlouvy, Speciálních podmínek, Podmínek platebního styku nebo VOP Klientem nebo Oprávněným uživatelem nebo nedodržením instrukcí předaných Bankou Klientovi nebo Oprávněnému uživateli.

8.8 Banka neodpovídá za škodu vzniklou dočasnou nedostupností služeb Internetového a Mobilního bankovnictví, poruchami datové, telefonní či mobilní sítě nebo poruchami nebo nedostupností služeb na straně mobilních operátorů nebo poskytovatelů internetového připojení.

9. REKLAMACE

Na uplatňování a řešení reklamací a stížností týkajících se provozu Internetového nebo Mobilního bankovnictví nebo chybně provedených Příkazů a jejich řešení se vztahují pravidla a lhůty uvedené v Reklamačním řádu Banky. Platný Reklamační řád je Klientům k dispozici na Internetových stránkách Banky a v Provozních prostorách Banky.

10. UKONČENÍ OBCHODNÍHO VZTAHU

10.1 Obchodní vztah mezi Bankou a Uživatelem může být ukončen jednostranně Bankou nebo Uživatelem podle jejich uvážení, není-li vzájemně dohodnuto jinak. Způsoby ukončení obchodního vztahu, výpovědní doby a další podrobnosti ukončení obchodního vztahu se řídí VOP, není-li v příslušné individuální smlouvě, Podmínkách platebního styku či těchto Speciálních podmínkách stanoveno jinak.

10.2 Smlouva zaniká zrušením účtu Klienta, ke kterému byla zřízena Přístupová práva. Pokud byla Přístupová práva zřízena k více účtům, zaniká Smlouva zrušením posledního z těchto účtů.

10.3 Uživatel i Banka jsou oprávněni Smlouvu písemně vypovědět. Podá-li výpověď Uživatel, zaniká Smlouva uplynutím výpovědní doby, která činí jeden měsíc ode dne doručení výpovědi Bance. Podá-li výpověď Banka, zaniká Smlouva uplynutím výpovědní doby, která činí dva měsíce a začíná běžet první den měsíce následujícího po odeslání výpovědi Uživateli.

10.4 Uživatel a Banka se mohou písemně dohodnout na ukončení Smlouvy ke sjednanému dni.

10.5 Banka je oprávněna písemně odstoupit od Smlouvy s okamžitou účinností, pokud Uživatel poruší nebo opakovaně porušuje podmínky příslušné Smlouvy nebo Speciálních podmínek, Podmínek platebního styku nebo VOP, nebo bezpečnostní instrukce Banky pro Uživatele týkající se užívání Internetového bankovnictví pro Uživatele, nebo i v dalších případech uvedených ve VOP.

11. PRAVIDLA BEZPEČNÉHO VYUŽÍVÁNÍ SLUŽEB A POVINNOSTI UŽIVATELE

11.1 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.

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

11.3 Uživatel je povinen chránit personalizované bezpečnostní prvky služeb Internetového bankovnictví (zejména Heslo, Bezpečnostní kód, MPIN a Biometrické údaje) před jejich ztrátou, odcizením nebo zneužitím.

11.4 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 Autorizačním telefonním číslem, 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 daly 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 bez zřejmé vazby ke své osobě nebo 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 pobočce 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 Internetových stránkách Banky v důvěryhodném prohlížeči nebo při přihlašování do Mobilní aplikace, 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 umístěný na jiném webu nesmí být využit); v souvislosti s uvedeným je také potřeba sledovat, zda prohlížeč před zadáním personalizovaných bezpečnostních prvků Internetového bankovnictví nehlásí bezpečnostní varování, např. ohledně důvěryhodnosti certifikátu SSL serveru; 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, 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);

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

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, 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;

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 Mobilní aplikace staženou pouze z oficiálních úložišť a zdrojů pro příslušný operační systém daného zařízení (Google Play, App Store); 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 Autorizačním telefonním číslem);

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

l) telefon s Autorizačním telefonním číslem 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;

m) mít zařízení využívané 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 zařízením;

n) zabezpečit zařízení využívané v souvislosti s Internetovým bankovnictvím biometrickým zabezpečením přístupu do zařízení, případně přístupovým kódem (číselným či grafickým) pro znemožnění užití 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 zařízení, u kterých byly provedeny úpravy označované jako root nebo jailbreak nebo jiné zásahy do software zařízení;

p) v případě, kdy je zařízení sloužící k přístupu do Internetového bankovnictví či telefon s Autorizačním telefonním číslem napaden škodlivým malwarem (ten může např. umožnit třetí osobě vzdáleně ovládat Internetové bankovnictví, vytěžit SMS s Bezpečnostním 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 Mobilní aplikaci, 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 Mobilní aplikace 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;

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 lince +420 583 037 060), 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.

11.5 Nedodržení opatření a postupů uvedených v předchozím bodě těchto Speciálních podmínek 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. 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.

11.6 V případě, že Bance vznikne podezření na neoprávněné nebo podvodné použití platebního prostředku informuje o tomto Banka Klienta způsobem uvedeným ve VOP.

12. ZÁVĚREČNÁ USTANOVENÍ

12.1 Banka je oprávněna tyto Speciální podmínky v souladu s článkem 44 VOP jednostranně měnit. Úpravy těchto Speciálních podmínek v případě technologických změn týkajících se přístupu do systému Internetového bankovnictví a jeho fungování a nezbytného zajištění kontinuity poskytování služeb Internetového bankovnictví ve vztahu k Uživatelům nebo v případě změny v rozsahu služeb poskytovaných v rámci Internetového bankovnictví jsou považovány za změny mechanického a administrativního rázu ve smyslu článku 44.5 VOP a nevyžadují pro účinnost změny předchozí oznámení Uživateli. Banka si dále vyhrazuje právo obdobně jednostranně změnit telefonní číslo Kontaktního centra a dobu, kdy je Kontaktní centrum k dispozici Uživatelům.

12.2 O veškerých změnách týkajících se Speciálních podmínek nebo fungování Kontaktního centra bude Banka Uživatele informovat vhodným způsobem (např. zprávou zaslanou službou Zprávy v rámci Internetového nebo Mobilního bankovnictví, prostřednictvím Internetových stránek Banky, informací na výpisu z účtu apod.).

12.3 Přechodná ustanovení

12.3.1 Podle znění těchto Speciálních podmínek účinných do 15. 11. 2025 bylo možno zřídit Internetové bankovnictví nebo ustanovit Oprávněného uživatele prostřednictvím Žádosti o zřízení přístupu do Internetového bankovnictví (dále jen „**Žádost**“). Žádost Klienta, kterou pro sebe zřídil přístup do Internetového bankovnictví, se považuje za Smlouvu ve smyslu těchto Speciálních podmínek. Přístupová oprávnění zřízená prostřednictvím Žádosti zůstávají nadále zachována. Oprávněnému uživateli, kterému byl zřízen přístup do Internetového bankovnictví na základě Žádosti ze strany jiného Klienta a sám dosud neuzavřel Smlouvu, zanikají Přístupová oprávnění z Žádosti, včetně samotného přístupu do Internetového bankovnictví, ke dni 30. 6. 2026, pokud do té doby neuzavře s Bankou Smlouvu.

12.3.2 Podle znění těchto Speciálních podmínek účinných do 15. 11. 2025 bylo možné ustanovit tzv. administrátora (dále jen „**Administrátor**“), což byl Oprávněný uživatel, kterému Klient v žádosti o zřízení nebo změnu přístupu k službám Internetového bankovnictví udělil plnou moc ke sjednávání produktů a služeb nabízených prostřednictvím Internetového bankovnictví. S účinností těchto Speciálních podmínek, tj. od 15. 11. 2025 se osoba Administrátora ruší a společně s tím se také ruší veškerá oprávnění, která byla v souvislosti s touto osobou v Bance vytvořena.

12.3.3 S účinností těchto Speciálních podmínek, tj. od 15. 11. 2025 budou dosavadní aplikace Internetového a Mobilního bankovnictví pod názvem Maxbanking nahrazeny novými aplikacemi pod názvem:

a) CREDITAS One – Internetové bankovnictví dostupné na adrese (URL) ib.maxbanka.eu

b) CREDITAS One Mobile – Mobilní bankovnictví dostupné prostřednictvím nové Mobilní aplikace s uvedeným názvem, která bude k dispozici v oficiálních zdrojích dle čl. 3.1.3 těchto Speciálních podmínek.

12.3.4 Pro přístup ke službám Internetového a Mobilního bankovnictví využije Uživatel své stávající bezpečnostní prvky, kterými se přihlašoval již před 15. 11. 2025. Při prvním přihlášení od 15. 11. 2025 je Uživatel povinen si Heslo změnit.

12.4 Zrušovací ustanovení

12.4.1 Tyto Speciální podmínky v den nabytí své účinnosti ruší a nahrazují dosavadní Obchodní podmínky pro využívání služeb Internetového bankovnictví Banky CREDITAS a.s. – Divize Max účinné od 01. 10. 2024.

12.5 Účinnost

12.5.1. Tyto Speciální podmínky jsou účinné ode dne 15. 11. 2025 za předpokladu, že Banka den účinnosti těchto Speciálních podmínek neposune na pozdější datum. Banka je oprávněna den účinnosti těchto Speciálních podmínek posunout ze závažných důvodů, přičemž informaci o této skutečnosti poskytne Klientům stejným způsobem, kterým oznámila návrh změny těchto Speciálních podmínek.