

**OBCHODNÍ PODMÍNKY BANKY CREDITAS A.S. PRO VYUŽÍVÁNÍ SLUŽEB INTERNETOVÉHO BANKOVNICTVÍ
– DIVIZE MAX**ÚČINNÉ OD ~~1. 10. 2024~~ 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	4
6.	PŘIJÍMÁNÍ PŘÍKAZŮ V RÁMCI PLATEBNÍCH SLUŽEB	6
7.	NEOBVYKLÉ UDÁLOSTI, PORUCHY INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ, SERVISNÍ SLUŽBY	7
8.	ODPOVĚDNOST KLIENTA	7
9.	REKLAMACE	8
10.	UKONČENÍ OBCHODNÍHO VZTAHU	8
11.	PRAVIDLA BEZPEČNÉHO VYUŽÍVÁNÍ SLUŽEB A POVINNOSTI UŽIVATELE	8
12.	ZÁVĚREČNÁ USTANOVENÍ	10

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 bankovníctví. tyto Obchodní podmínky Banky CREDITAS a.s. pro používání služeb Internetového bankovníctví – 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 přímému Internetovému bankovníctví, 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, resp. nebo výše v textu těchto Speciálních podmínek nebo ve VOP:

Administrátor – Oprávněný uživatel, kterému Klient v žádosti o zřízení nebo změnu přístupu k službám Internetového bankovníctví udělil plnou moc ke sjednávání produktů a služeb nabízených prostřednictvím Internetového bankovníctví;

Autorizační telefonní číslo – unikátní mobilní telefonní číslo s českou nebo slovenskou předvolbou, které má Uživatel sjednané s Bankou pro účely využívání služeb Internetového bankovníctví. Uživatel může mít pouze jedno Autorizační telefonní číslo. Změnu Autorizačního telefonního čísla může Uživatel provést prostřednictvím Internetového nebo Mobilního bankovníctví, 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 47623903;

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

Bezpečnostní kód – při SMS přístupu kód, zaslaný Bankou Klientovi Uživateli SMS zprávou vždy na Autorizační telefonní číslo, sloužící pro potvrzení změny, přístupového hesla při prvním přihlášení, přístup Uživatele do Internetového bankovníctví nebo při každé další změně Hesla nebo pro podpis platebního příkazu nebo zprávy zasílané Klientem Bance prostřednictvím autorizaci platebních příkazů a operací prováděných Uživatелеm v rámci Internetového bankovníctví;

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

Denní limit pro platební operace – maximální denní limit v CZK do kterého je možné provádět platby z účtu/účtů klienta

ePIN kód – je osobní identifikační číslo (pokud je Bankou držiteli karty zpřístupněn), zpřístupněné pouze držiteli karty a používané výhradně k autorizaci 3D-Secure zabezpečených platebních transakcí provedených platební kartou;

Heslo – řetězec písmen, číslic a/nebo znaků umožňující SMS-přístup a přístup s GA kódem do Internetového bankovníctví;
Informační služby a Nastavení – služby poskytované Bankou prostřednictvím Internetového bankovníctví uvedené v článku 4.1 těchto Speciálních podmínek;

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 veden Bankou, Klientovi prostřednictvím Banky jako poskytovatele služby Informování o platebním účtu;

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

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

Klient – majitel účtu u Banky, který s Bankou uzavírá příslušnou Smlouvu a určuje Oprávněné uživatele/u Internetového bankovníctví;

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 bankovníctví prostřednictvím Mobilních mobilních zařízení;

Mobilní bankovníctví – Internetové bankovníctví 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 veden Bankou, Klientem prostřednictvím Banky jako poskytovatele služby nepřímého dání platebního příkazu;

Notifikace – vyžádané SMS, ~~nebo emailové-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 bankovníctví;

PIN—osobní identifikační kód Klienta, sloužící k ověření totožnosti osoby zadávající tento kód;

Platební služby—služby poskytované Bankou prostřednictvím Internetového bankovníctví uvedené v článku 4.2 těchto Speciálních podmínek;

Příkaz – příkaz nebo žádost zadaná Klientem/Uživatелеm Bance prostřednictvím Internetového nebo Mobilního bankovníctví v rámci Platebních služeb;

Přístupová oprávnění – soubor autorizačních oprávnění, vymezující účty a jiné služby, s nimiž bude disponováno a jež budou užívány prostřednictvím Internetového nebo Mobilního bankovníctví, 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 bankovníctví uzavřená mezi Bankou a Klientem/Uživatелеm, případně jiná smlouva v rozsahu platného ujednání o přístupu Klienta/Uživatele do Internetového bankovníctví na základě takové smlouvy;

SMS přístup—přístup do Internetového bankovníctví s možností využívat Informační služby i Platební služby. Tento přístup lze zřídit k mobilním číslům tuzemských a zahraničních Mobilních operátorů;

Speciální podmínky—tyto obchodní podmínky Banky pro používání služeb Internetového bankovníctví, vydané jako doplněk k VOP a Podmínkám platebního styku;

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

Uživatel – fyzická osoba, Klient nebo Oprávněný uživatel Internetového a Mobilního bankovníctví s definovanými Přístupovými oprávněními k účtům a produktům Klienta;

Uživatelské jméno – uživatelské jméno, pod kterým se Klient/Uživatel hlásí do Internetového bankovníctví;

VOP—Všeobecné obchodní podmínky Banky CREDITAS a.s.—Divize Max;

Zákaznické centrum—zákaznické servisní a kontaktní centrum Banky, poskytující přístup k vybraným službám Banky prostřednictvím prostředků vzdálené komunikace, dostupné na kontaktních údajích zveřejněných na Internetové stránce Banky.

3. PŘEDPOKLADY PRO POUŽÍVÁNÍ INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ

3.1 Technické požadavky pro Internetové a Mobilní bankovníctví:

Technické požadavky pro používání Internetového a Mobilního bankovníctví jsou dostupné na internetových stránkách Banky CREDITAS a.s. – Divize Max: www.maxbanka.eu. Klient/Uživatel se zavazuje se s technickými požadavky a opatřeními seznámit a řídit se jimi.

3.1.1 Hardware – klientská stanice pro Internetové bankovníctví 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 bankovníctví je potřeba mít na svém mobilním zařízení nainstalovanou Mobilní aplikaci, kterou lze stáhnout u poskytovatele aplikací dle operačního systému mobilního zařízení Klienta/Uživatele. Mobilní aplikace je Bankou distribuována prostřednictvím oficiálních zdrojů Google Play, a App Store ~~a Huawei AppGallery~~. Klient je povinen neinstalovat Mobilní aplikaci z jiných než z těchto oficiálních zdrojů.

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

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

4. ~~PŘEHLED HLAVNÍCH SLUŽEB POSKYTOVANÝCH~~DORUČOVÁNÍ A KOMUNIKACE PROSTŘEDNICTVÍM INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ

4.1 ~~Informační služby a Nastavení poskytované v Internetovém bankovníctví:~~

(a) ~~Přehled účtů Klienta~~

(b) ~~Zobrazení detailů účtů Klienta~~

(c) ~~Stav aktuálních zůstatků na účtech Klienta~~

(d) ~~Výpis transakční historie na účtech Klienta~~

(e) ~~Výpisy z účtů klienta ve formátu PDF~~

(f) ~~Zprávy – Služba umožňující oboustranné zasílání textových zpráv. Ke zprávě může být přiložena příloha (soubor)~~

(g) ~~Změna hesla pro přihlašování do Internetového bankovníctví~~

(h) ~~Nastavení notifikací – SMS zprávy nebo emaily, kterými banka informuje Klienta o operacích souvisejících s produkty Klienta~~

- (i) ~~Přehled investičních produktů~~
- (j) ~~Přehled úvěrových produktů~~
- (k) ~~Přehled a správa třetích stran~~
- (l) ~~Nadstavbové služby k vybraným účtům~~

4.2 Platební služby

- (a) ~~Tuzemské platební příkazy — Banka přijímá platební příkazy zadané Klientem interně v rámci Banky i mimo Banku v rámci České republiky, kde měna účtů a převodu může být v českých korunách, nebo jiných měnách.~~
- (b) ~~Zahraniční platební příkazy — Banka přijímá platební příkazy interně v rámci Banky, do zahraničí, i v rámci České republiky v českých korunách, nebo jiných měnách.~~
- (c) ~~Platby mezi vlastními účty ve měně jednoho z účtů převodu bez nutnosti autorizace platby~~
- (d) ~~SEPA platební příkazy — Banka přijímá platební příkazy SEPA ve měně EUR interně v rámci Banky a do zemí EU/EHP.~~
- (e) ~~Povolení k inkasu / SIPO ve prospěch jiného účtu v rámci České republiky~~
- (f) ~~Nastavení domácích a zahraničních trvalých příkazů~~

4.3 Karotní služby

- (a) ~~Zobrazení transakcí provedených platební kartou~~
- (b) ~~Zobrazení informací o limitech a možnost změny limitů karty~~
- (c) ~~Možnost aktivace pojištění k platební kartě~~
- (d) ~~Blokace karty~~
- (e) ~~Nastavení PIN kódu k platební kartě~~
- (f) ~~Nastavení telefonního čísla a ePIN pro službu 3D Secure k platební kartě~~
- (g) ~~Žádost o vydání nové platební karty~~
- (h) ~~Blokace transakcí s využitím Dynamic Currency Conversion (DCC)~~
- (i) ~~Blokace transakcí pomocí magnetického proužku~~
- (j) ~~Blokace transakcí na bankomatech, kdy je účtován surcharge poplatek~~
- (k) ~~Blokace zobrazení zůstatku v bankomatu a internetovém bankovníctví~~

4.4.1 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 aplikaci Internetového nebo Mobilního bankovníctví. 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 bankovníctví. Banka a Klient se dále dohodli, že Banka je oprávněna jednostranně neakceptovat dokumenty doručené Klientem prostřednictvím Internetového nebo Mobilního bankovníctví, přičemž Banka tak může učinit bez udání důvodu. V případě, že Banka neakceptuje dokumenty, které jí zaslal Klient prostřednictvím Internetového nebo Mobilního bankovníctví, pak o takové skutečnosti Klienta vyrozumí. Banka se s Klientem dohodla, že dokumenty, které Klient zašle prostřednictvím Internetového nebo Mobilního bankovníctví Bance, budou ve formátu pdf.

4.5.2 Vzájemná komunikace

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

4.6.3 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 bankovníctví, kde vlastnoruční podpis Klienta bude nahrazen elektronickým podpisem spočívajícím v ~~odeslání Autorizačního kódu Bance zadání obdrženého Bezpečnostního kódu nebo MPINU~~ pomocí elektronického úkonu učiněného Klientem v Internetovém nebo Mobilním bankovníctví. Takový způsob právního jednání bude Klientovi umožněn pouze v případech stanovených Bankou.

4.7.4 Mobilní bankovníctví

Mobilní bankovníctví umožňuje přihlašování, autorizaci platebních příkazů a požadavků ~~zadaných prostřednictvím Internetového bankovníctví~~ a ovládání účtů vedených Bankou v ~~rozsahu~~ v jakém to ~~Mobilní aplikace Mobilního bankovníctví~~ umožní.

5. PŘÍSTUP DO INTERNETOVÉHO A MOBILNÍHO BANKOVNICTVÍ

~~5.1 Služby Internetového a Mobilního bankovníctví poskytuje Banka pouze Klientovi, který má veden účet, nebo jiný produkt umožňující využití přístupu Internetového nebo Mobilního bankovníctví a uzavřel s Bankou příslušnou Smlouvu a jím zmocněným Oprávněným uživateli, přičemž Oprávněným uživateli Banka umožňuje přístup do Internetového bankovníctví pouze v rozsahu Přístupových oprávnění určených Klientem.~~

~~5.1 Banka na základě Smlouvy umožní Uživateli prostřednictvím Internetového a Mobilního bankovníctví 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 Klientem Uživatel a Bankou může být uzavřena prostřednictvím Internetového bankovníctví, ~~případně prostřednictvím online registrace na Internetových stránkách Banky~~, korespondenčně s úředně ověřeným podpisem nebo osobně po ověření pracovníkem Banky.
- ~~5.3 Nodílnou součástí Smlouvy je Žádost o zřízení nebo změnu přístupu k službám Internetového bankovníctví („Žádost“). Řádně vyplněnou a podepsanou Žádost je Klient povinen předat Bance osobně nebo zaslat s úředně ověřeným podpisem Bance případně prostřednictvím Internetového bankovníctví, pokud to Banka Klientovi umožní. Na základě Žádosti zřizuje Banka Klientovi jednotlivá Přístupová práva k určeným produktům, účtům a v určeném rozsahu, včetně Přístupových práv pro Oprávněné uživatele (Disponenty). Žádost je rovněž podkladem pro provedení změn v existujících Přístupových oprávněních nebo zřízení nového Přístupového oprávnění. Přístupová práva pro Oprávněné uživatele (Disponenta) může Klient zřídit a měnit i prostřednictvím Internetového bankovníctví.~~
- ~~5.4. Přístupové oprávnění pro Oprávněné uživatele může vlastník účtu~~ 5.3. Přístupové oprávnění pro Oprávněné uživatele může Klient zřídit, změnit nebo odebrat prostřednictvím Internetového bankovníctví, korespondenčně s úředně ověřeným podpisem ~~případně osobně po ověření pracovníkem Banky~~. Vlastník účtu může na základě plné moci, pověřit i jiné oprávněné uživatele, kteří budou provádět správu Oprávněných uživatelů prostřednictvím Internetového bankovníctví. Přístupová oprávnění udělená Oprávněnému uživateli lze také kdykoli zrušit písemným pokynem Klienta Bance, ~~případně osobně po ověření pracovníkem Banky~~.
- ~~5.5 Klient a Oprávněný uživatel jsou oprávněni~~ 5.4 Uživatel je oprávněn pracovat s Internetovým a Mobilním bankovníctvím dvacet čtyři (24) hodin denně. Banka je oprávněna omezit či přerušit provoz Internetového a Mobilního bankovníctví na dobu nezbytně nutnou pro jeho údržbu.
- Přístup do Internetového bankovníctví:**
- ~~5.6 Pokud ze Smlouvy nevyplývá jinak, Banka zřizuje Klientovi a Oprávněnému uživateli pouze SMS přístup.~~

SMS přístup:

- 5.7 Při **SMS** přístupu do Internetového bankovníctví se za účelem identifikace 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 bankovníctví 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 ~~se přihlašujícím~~ samostatně na dokumentu neprodleně po uzavření Smlouvy na Provozně 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 bankovníctví svým Uživatelským jménem, Heslem, které si Uživatel sám zvolí, a dynamicky generovaným Bezpečnostním kódem zaslaným jeho prostředím změnit;
- b) Bezpečnostního kódu:
Bezpečnostní kód pro přihlášení je zasílán Uživateli Bankou prostřednictvím SMS zprávy po zadání přihlašovacího jména v rámci prostředí Internetových stránek Banky určeného pro přihlášení do Internetového bankovníctví.
V některých případech vyžaduje přihlášení do Internetového bankovníctví také za dání data narození. Namísto Bezpečnostního kódu a Hesla může být Uživatel využívá Mobilní aplikace instalovaná na mobilním zařízení Uživatele, která umožňuje Uživateli použít k přihlášení ~~namísto Bezpečnostního kódu PIN~~ MPIN kód Mobilní aplikace (který si volí Uživatel) či Biometrický údaj Uživatele.
- ~~5.8 Pro zřízení SMS přístupu zasílá Banka Uživateli SMS zprávu s Jednorázovým Heslem na Klientem určené telefonní číslo. Jednorázové Heslo slouží jako Heslo pouze pro první přihlášení do Internetového bankovníctví, po kterém je Uživatel povinen provést změnu Hesla. První a jakoukoliv další změnu Hesla musí Uživatel potvrdit zadáním Bezpečnostního kódu, který mu bude po zadání této změny zaslán SMS zprávou na jím předem určené telefonní číslo. Heslo zvolené Uživatelem zůstane v platnosti až do jeho další změny, která probíhá již pouze z iniciativy Uživatele. Banka doporučuje provádět změnu Hesla alespoň jednou měsíčně.~~
- ~~5.9 Při další autentizaci Uživatele do Internetového bankovníctví může být kombinace Hesla a Bezpečnostního kódu nahrazena přihlášením prostřednictvím autentizace v Mobilní aplikaci po načtení přihlašovacího QR kódu.~~
- 5.7 Pro autorizaci ~~přihlášení~~, platebního příkazu, nebo jiného požadavku realizovatelného prostřednictvím Internetového bankovníctví či Mobilního bankovníctví Uživatel obdrží od Banky prostřednictvím SMS zprávy Bezpečnostní kód, jehož zadáním příslušný platební příkaz, ~~přihlášení~~ nebo jiný požadavek autorizuje. Namísto použití Bezpečnostního kódu může Uživatel autorizovat ~~přihlášení~~, platební příkaz či jiný požadavek realizovatelný prostřednictvím Internetového bankovníctví či Mobilního bankovníctví zadáním ~~PIN~~ MPIN kódu Mobilní aplikace (který si volí Uživatel) v Mobilní aplikaci instalované na mobilním zařízení Uživatele či prostřednictvím Biometrického údaje nastaveného tamtéž. U vybraných požadavků může Banka umožnit jejich autorizaci pouhým kliknutím na odpovídající potvrzovací tlačítko v Internetovém bankovníctví. Banka si vyhrazuje právo u vybraných požadavků umožnit pouze jí určený způsob autorizace.

- 5.105.8** 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 přerušeno telekomunikačního spojení nebo v důsledku technické závady na přenosových zařízeních.
- 5.115.9** Uživatel může používat oba způsoby autorizace (Bezpečnostní kód a Mobilní aplikaci) souběžně. Podmínkou pro využívání Mobilní aplikace je její úspěšná registrace.

Přístup do Mobilního bankovníctví:

5.175.10 Do Mobilního bankovníctví se Uživatel přihlašuje zadáním PIN-kóduMPIN nebo Biometrickým údajem. Pro registraci (aktivaci) Mobilní aplikace ~~pro autorizaci platebních příkazů, přihlašování do Internetového a Mobilního bankovníctví a dalších požadavků~~ je podmínkou ověření identity Uživatele, a to prostřednictvím ~~kódu získaného v Internetovém bankovníctví a zadáním hesla pro Internetové bankovníctví, nebo ověřením identity prostřednictvím~~ Uživatelského jména a ~~hesla pro Internetové bankovníctví. V obou případech je třeba ověření identity potvrdit, data narození, Hesla a potvrzením~~ Bezpečnostním kódem. V případě použití jednorázového hesla je ~~uživatel~~po Uživateli v průběhu registrace ~~umožněno vyžadováno~~ nastavení nového hesla pro Internetové bankovníctví. ~~V případě opakovaně chybného ověření identity Uživatele dojde k automatickému zablokování Uživateleova přístupu do Internetového bankovníctví a do Mobilní aplikace.~~

5.11 ~~Autorizaci platebního příkazu nebo jiného požadavku realizovatelného prostřednictvím Mobilního bankovníctví Uživatel v takovém případě musí kontaktovat zákaznické centrum Banky, kde mu po náležité identifikaci příslušný pracovník Banky přístup odblokuje provádí zadáním MPIN kódu nebo Biometrickým údajem. U vybraných požadavků může Banka umožnit jejich autorizaci pouhým kliknutím na odpovídající potvrzovací tlačítko v Mobilním bankovníctví. Banka si vyhrazuje právo u vybraných požadavků umožnit pouze jí určený způsob autorizace.~~

5.18 ~~Uživatel je povinen chránit zařízení, ve kterém je nainstalována Mobilní aplikace, před ztrátou a zneužitím cizí osobou. Na mobilním zařízení (zejména tzv. smartphony a tablety) s operačním systémem iOS, Android a jiným operačním systémem, na kterých se používá Internetové nebo Mobilní bankovníctví nebo je v nich SIM karta obsahující telefonní číslo určené k přijímání sms zpráv od Banky, je Uživatel povinen neinstalovat aplikace z jiných než oficiálních zdrojů pro příslušný operační systém mobilního zařízení (např. App Store, Google Play, Huawei AppGallery atd.). Banka dále Klienta upozorňuje, že Klient nemůže spoléhat na kontrolu prováděnou provozovatelem operačního systému ve vztahu ke všem aplikacím.~~

6. PŘIJÍMÁNÍ PŘÍKAZŮ V RÁMCI PLATEBNÍCH SLUŽEB

- 6.1** Banka zpracovává zaslané Příkazy pouze do času uzávěrek. Časy uzávěrek jsou vyhlášovány Bankou a jsou k dispozici Klientovi na ZákaznickémKontaktním centru a případně též na ~~internetových~~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** ~~V rámci Informačních služeb Banka poskytuje Klientovi informace umožňující identifikovat transakci, výši částky v měně, ve které je účtováno, případně také v měně Příkazu a použitý směnný kurz. 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 bankovníctví může Banka stanovit maximální denní limit pro převody peněžních prostředků. ~~Limit je specifikován v Žádosti.~~ Tento limit může být stanoven po dohodě s Klientem nebo jednostranně Bankou. ~~Při SMS přístupu do systému Internetového bankovníctví hrozí vyšší riziko jeho možného zneužití a vzniku škody a pokud Klient požaduje vyšší limit, než který mu pro tento typ přístupu navrhne Banka, Klient toto zvýšené riziko bere na vědomí a přijímá.~~ 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 zasláného 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 ~~Klient i Oprávněný uživatel jsou povinni~~ Uživatel je povinen bez zbytečného odkladu oznámit Bance jakoukoliv poruchu Internetového nebo Mobilního bankovníctví včetně jejího popisu.
- 7.2 V případě, že Uživatel pro vstup do Internetového bankovníctví použije opakovaně chybné přihlašovací údaje, nebo Bezpečnostní kód, dojde k automatickému dočasnému zablokování Uživatelova přístupu do Internetového bankovníctví. ~~Uživatel musí kontaktovat zákaznické centrum banky, kde mu po identifikaci příslušný pracovník přístup odblokuje.~~ V případě, že Uživatel při autorizaci opakovaně zadá chybný PINMPIN v Mobilní aplikaci, bude Mobilní aplikace automaticky odregistrována a je třeba provést opětovnou registraci.
- 7.3 Banka je oprávněna zablokovat přístup ~~Klienta a Oprávněného uživatele~~ Uživatele do Internetového a Mobilního bankovníctví, 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 bankovníctví bude ~~Klientovi a Oprávněnému uživateli~~ Uživateli obnoveno až poté, co pomine nebezpečí jeho zneužití, případně po přijetí nezbytných opatření. ~~Klient nebo Oprávněný uživatel~~ Uživatel je oprávněn požádat Banku o zablokování přístupu do Internetového nebo Mobilního bankovníctví. Zablokováním přístupu do Internetového nebo do Mobilního bankovníctví budou přerušeny služby Třetích stran.
- 7.4 Banka si vyhrazuje právo jednostranně bezplatně změnit ~~Klientovi a Oprávněnému uživateli~~ Uživateli používaný typ přístupu do Internetového a Mobilního bankovníctví na přístup poskytující vyšší stupeň zabezpečení.

8. ODPOVĚDNOST KLIENTA

- ~~8.1 Klient a každý Oprávněný uživatel jsou povinni chránit svá přístupová data, tj. Uživatelské jméno a Heslo pro SMS přístup, SIM kartu, na kterou jsou mu zaslány Heslo a Bezpečnostní kód, PIN kód Mobilní aplikace, Bezpečnostní kódy a přístupové údaje ke své e-mailové adrese používané v souvislosti internetovým bankovníctvím před jejich ztrátou nebo zneužitím, uchovávat je v tajnosti a nesdělovat je žádné třetí osobě. Klient i každý Oprávněný uživatel jsou povinni Banku bez zbytečného odkladu informovat o jejich ztrátě nebo o podezření na jejich zneužití prostřednictvím Zákaznického centra na telefonních číslech 800 700 800 nebo +420 233 233 233 (nonstop), která jsou k dispozici také na www.maxbanka.eu. Banka nenes odpovědnost za škodu, kterou utrpí Klient či Oprávněný uživatel v důsledku ztráty přístupových dat nebo jejich zneužití, o nichž nebude Banka Klientem či Oprávněným uživatelem bez zbytečného odkladu informována.~~

8.1 Úmyslně vynecháno

- 8.2 Klient bere na vědomí, že v případě SMS-přístupu do Internetového bankovníctví Heslo a Bezpečnostní kód a pro Mobilní aplikaci PINMPIN kód nebo Biometrický údaj, slouží k ověření jeho totožnosti, resp. totožnosti Oprávněného uživatele pro přístup do Internetového bankovníctví.
- 8.3 Transakce a úkony autorizované Bezpečnostním kódem a pro Mobilní aplikaci PINMPIN 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 AutorizačníhoMPIN kódu ~~nebo~~, Bezpečnostního kódu nebo Biometrickým údajem.

- ~~8.4 Klient je povinen neprozrazovat žádné skutečnosti týkající se technického a organizačního zajištění bezpečnosti a prevence zneužití Internetového a Mobilního bankovníctví a okamžitě informovat Banku, dojde-li ke ztrátě nebo vyzrazení jeho přístupových dat nebo přístupových dat Oprávněného uživatele, zejména Hesla nebo PIN kódu, nebo pokud má podezření, že došlo ke zneužití jeho přístupu do Internetového a Mobilního bankovníctví. Současně je povinen zajistit dodržování výše uvedeného Oprávněným uživatelem.~~

- ~~8.5 Banka zablokuje přístup na Klientovy účty prostřednictvím Internetového bankovníctví, pokud dojde k jeho zneužití nebo pokud Klient oznámí ztrátu nebo vyzrazení přístupových dat nebo podezření, že by mohlo dojít ke zneužití přístupu. O zablokování přístupu bude Banka Klienta informovat bez zbytečného prodlení. Přístup do Internetového bankovníctví bude Klientovi obnoven až poté, co pomine nebezpečí jeho zneužití.~~

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 (pět) 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 Pokud v souvislosti s využíváním Internetového bankovníctví použijete aplikaci třetí strany, pak Banka neodpovídá za použití takové aplikace, ani za informace, které obdržíte jejím prostřednictvím.~~
- ~~8.8 Banka neodpovídá za škodu vzniklou dočasnou nedostupností služeb Internetového a Mobilního bankovníctví, 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 bankovníctví nebo chybně provedených Příkazů a jejich řešení se vztahují pravidla a lhůty uvedené v Reklamačním řádu Banky, kteřý: Platný Reklamační řád je zveřejněn Klientům k dispozici na Internetových stránkách Banky a v Provozních prostorách Banky.

10. UKONČENÍ OBCHODNÍHO VZTAHU

- 10.1 Obchodní vztah mezi Bankou a KlientemUživatелеm může být ukončen jednostranně Bankou nebo KlientemUživatелеm 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 KlientUživatel i Banka jsou oprávněni Smlouvu písemně vypovědět. Podá-li výpověď KlientUživatel, 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 KlientoviUživateli.
- 10.4 KlientUživatel 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 KlientUživatel poruší nebo opakovaně porušuje podmínky příslušné Smlouvy nebo Speciálních podmínek, Podmínek platebního styku nebo VOP, nebo bezpečnostní instrukce Banky pro KlientaUživatele týkající se užívání Internetového bankovníctví pro KlientaUživatele, 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 bankovníctví a poskytování služeb Nepřímého dání platebního příkazu a Informování o platebním účtu.
- 11.2 Ustanovení tohoto článku shrnují základní pravidla bezpečného využívání služeb Internetového bankovníctví, Nepřímého dání platebního příkazu a Informování o platebním účtu.
- 11.3 Uživatel je povinen chránit personalizované bezpečnostní prvky služeb Internetového bankovníctví (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 bankovníctví a dalších důvěrných informací v rámci Internetového bankovníctví, která jsou s ohledem na obvyklá rizika porušení ochrany důvěrných informací technicky možná a přiměřená, a dále také zajistit bezpečnost zařízení pro využití Internetového bankovníctví 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 bankovníctví, neukládat je na žádné trvalé nosiče dat, případně je uschovávat 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 bankovníctví před jinou osobou, nesdělovat personalizované bezpečnostní prvky Internetového bankovníctví jiným osobám, a to ani rodinným příslušníkům a osobám blízkým; dále neumožnit automatické zapamatování personalizovaných bezpečnostních prvků Internetového bankovníctví pro přístup do Internetového bankovníctví, obzvláště pokud komunikační zařízení využívá více osob;
- c) stanovit volitelné personalizované bezpečnostní prvky Internetového bankovníctví 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 bankovníctví výhradně na pobočce Banky anebo prostřednictvím Internetového bankovníctví, nebo jiným bezpečným způsobem předem dohodnutým s Bankou; změnit si volitelné personalizované bezpečnostní prvky Internetového bankovníctví okamžitě při podezření na jejich vyzrazení;
- e) nezasílat personalizované bezpečnostní prvky Internetového bankovníctví 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 Uživatелеm 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 bankovníctví třetí osobě, a musí ihned danou situaci konzultovat s Bankou;

- f) žadávat personalizované bezpečnostní prvky služeb Internetového bankovníctví 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 bankovníctví odkazů otevíraných ze sociálních sítí, e-mailů, SMS, aplikací pro vzájemnou komunikaci, internetových vyhledávačů, ani proklikem přes zobrazené sponzorované odkazy; přihlašovací formulář do Internetového bankovníctví umístěný na jiném webu nesmí být využit); v souvislosti s uvedeným je také potřeba sledovat, zda prohlížeč před zadáním personalizovaných bezpečnostních prvků Internetového bankovníctví 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 bankovníctví jen na zařízeních a v sítích, které jsou důvěryhodné a řádně zabezpečené proti zneužití důvěrných informací; Uživatel nesmí používat Internetové bankovníctví 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 bankovníctví Uživatel nesmí využívat nezabezpečenou, veřejně přístupnou síť (např. nezabezpečenou wifi síť v ubytovacích zařízeních, restauracích, veřejných prostranstvích);
- h) bezprostředně po ukončení práce s Internetovým bankovníctvím 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 bankovníctví nebo zavřením Mobilní aplikace neponechávat dané zařízení bez dohledu;
- i) legálně zabezpečit zařízení pro využití Internetového bankovníctví (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 bankovníctví, 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 bankovníctví 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 úložiště – 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 bankovníctví či do telefonu s Autorizačním telefonním číslem);
- k) v případě nedostatečné znalosti nastavení zabezpečení zařízení pro využití Internetového bankovníctví 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 bankovníctvím technologicky chránit obdobně jako zařízení pro využití služeb Internetového bankovníctví (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 bankovníctvím 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 bankovníctvím 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 bankovníctví 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 bankovníctví či telefon s Autorizačním telefonním číslem napaden škodlivým malwarem (ten může např. umožnit třetí osobě vzdáleně ovládat Internetové bankovníctví, 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 bankovníctví, a to v případě potřeby i opakovaně;

- q) pozorně číst oznámení zasláná 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 bankovníctví, změně kontaktního e-mailu či o aktivaci digitální peněženky, a bezodkladně o tom informovat Banku; Bankou zasláné 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 bankovníctví nebo chybu, ztrátu, odcizení či zneužití platebního prostředku či ve vztahu k personalizovaným bezpečnostním prvkům Internetového bankovníctví (např. zničení, ztráta nebo odcizení zařízení pro využití Internetového bankovníctví anebo telefonu využívaného v souvislosti s Internetovým bankovníctvím či jejich napadení virem) anebo k zaslání 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 bankovníctví; 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 bankovníctví 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 bankovníctví nebo dalších důvěrných informací v rámci Internetového bankovníctví 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

4412.1 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 bankovníctví a jeho fungování a nezbytného zajištění kontinuity poskytování služeb Internetového bankovníctví ve vztahu ~~ke Klientům~~ Uživatelům nebo v případě změny v rozsahu služeb poskytovaných v rámci Internetového bankovníctví jsou považovány za změny mechanického a administrativního rázu ve smyslu článku 44.5 VOP a nevyžadují pro účinnost změny předchozí oznámení ~~Klientovi~~ Uživateli. Banka si dále vyhrazuje právo obdobně jednostranně změnit telefonní číslo ~~Zákaznického~~ Kontaktního centra a dobu, kdy je ~~Zákaznické~~ Kontaktní centrum k dispozici ~~Klientům~~ Uživatelům.

4412.2 O veškerých změnách týkajících se Speciálních podmínek nebo fungování ~~Zákaznického~~ Kontaktního centra bude Banka ~~Klienta~~ Uživatele informovat vhodným způsobem (např. zprávou zaslou službou Zprávy v rámci Internetového nebo Mobilního bankovníctví, prostřednictvím Internetových stránek Banky, informací na výpisu z účtu apod.).

12.3 Přejícná ustanovení

12.3.1 Podle znění těchto Speciálních podmínek účinných do 15. 11. 2025 bylo možno zřídit Internetové bankovníctví nebo ustanovit Oprávněného uživatele prostřednictvím Žádosti o zřízení přístupu do Internetového bankovníctví (dále jen „Žádost“). Žádost Klienta, kterou pro sebe zřídil přístup do Internetového bankovníctví, 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 bankovníctví na základě Žádosti ze strany jiného Klienta a sám dosud neuzavřel Smlouvu, zanikají Přístupová oprávnění z Žádosti, včetně samotného přístupu do Internetového bankovníctví, 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 bankovníctví udělil plnou moc ke sjednávání produktů a služeb nabízených prostřednictvím Internetového

bankovníctví. 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 bankovníctví pod názvem Maxbanking nahrazeny novými aplikacemi pod názvem:

a) CREDITAS ON – Internetové bankovníctví dostupné na adrese (URL) ib.maxbanka.eu

b) CREDITAS ON Mobile – Mobilní bankovníctví 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 bankovníctví 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 ~~ke dni 1.10. 2024~~ ruší a nahrazují dosavadní Obchodní podmínky pro využívání služeb Internetového bankovníctví ~~Max banky a.s.~~ 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.

Tyto Obchodní podmínky pro využívání služeb Internetového bankovníctví jsou platné ode dne 1. 10. 2024 (dále jen „datum vyhlášení“) a účinné od data vyhlášení ve vztahu k novým Klientům. Ve vztahu ke stávajícím Klientům Banky, kteří vstoupili do smluvního vztahu s Bankou před datem vyhlášení, nabývají tyto Obchodní podmínky pro využívání služeb Internetového bankovníctví účinnosti ~~ke dni 1.10. 2024~~ a nahrazují dosavadní Obchodní podmínky pro využívání služeb Internetového bankovníctví ~~Max banky a.s.~~