Pravidla bezpečného používání internetového bankovnictví

Platné od 2. 9. 2024

Účelem tohoto dokumentu je poskytnout Vám před uzavřením rámcové smlouvy a zejména smlouvy umožňující využívat služby internetového bankovnictví informace podle ust. § 133 a 134 až 139 zákona č. 370/2017 Sb. o platebním styku.

Poskytovatelem služeb internetového bankovnictví je UniCredit Bank Czech Republic and Slovakia, a.s., se sídlem Želetavská 1525/1, 140 92 Praha 4 – Michle, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 3608, IČO 64948242 (dále jen „UniCredit Bank"), tel. +420 221 210 031, e-mail: info@unicreditgroup.cz. Nad činností UniCredit Bank vykonává dohled Česká národní banka se sídlem v Praze, doručovací adresa Na Příkopě 28, 115 03 Praha.

Jako klient/uživatel můžete v rámci internetového bankovnictví v aplikaci Smart Banking nebo Online Banking prostřednictvím sítě internet využívat určité bankovní služby, komunikovat s UniCredit Bank sjednaným způsobem a zejména autorizovat příslušné platební transakce nebo jiné pokyny. Každé Vaše potvrzení, souhlas či jiné jednání obdobné povahy učiněné v internetovém bankovnictví při použití příslušného osobního bezpečnostního prvku je považováno za Váš závazný projev vůle.

1. Osobní bezpečnostní prvky sloužící pro ověření uživatele (dále jen „bezpečnostní prvky")

Prvky sloužící pro Vaše ověření jsou jedinečné bezpečnostní prvky, které Vám umožňují vstupovat do internetového bankovnictví a využívat produkty aplikací Smart Banking nebo Online Banking včetně ověření totožnosti uživatele prostřednictvím bankovní identity Bank iD. Tyto prvky jsme Vám buď přidělili, nebo jste si je sami zvolili. Každý prvek je určitého typu:

a) Znalost (Z) – tzn. něco, co jenom uživatel zná.
b) Vlastnictví (V) – tzn. něco, co jenom uživatel má.
c) Inherence/Biometrie (I) – něco, čím uživatel je (unikátní údaj o uživateli).

Pokud jsou pro ověření použity minimálně 2 prvky, přičemž každý musí být z jiné kategorie, jedná se o tzv. „silné ověření klienta".

Osobní bezpečnostní prvky jsou:

Prvek	Popis	Typ
PIN pro mobilní aplikaci	Číselný kód pro mobilní aplikaci Smart Banking, který se používá při aktivaci, přihlášení nebo pro potvrzování transakcí. Tento PIN je nepřenosný, nastavuje si ho sám uživatel a **smí ho znát pouze uživatel** (podobně jako PIN k platební kartě). Tento PIN se používá pouze v aplikaci Smart Banking.	Z
Heslo	Heslo se skládá z numerických znaků (délka 6 znaků). Používá se pro přihlášení do internetového bankovnictví Online Banking (v kombinaci s jednorázovým SMS kódem). Heslo je nepřenosné a smí ho znát pouze uživatel. Úvodní heslo si musí uživatel ihned změnit na své. Heslo se používá pouze v aplikaci Online Banking (na adrese cz.unicreditbanking.eu).	Z
Aktivovaná mobilní aplikace (SW bezpečnostní klíč)	Mobilní aplikace Smart Banking v sobě obsahuje „bezpečnostní klíč" (Smart klíč). Po aktivaci je aplikace jednoznačně spojena s uživatelem. Aplikace umožňuje přijímat push-notifikační zprávy, jejichž pomocí je možno potvrdit přihlášení do aplikace Online Banking nebo autorizovat platební transakci. Aplikace umožňuje generovat jednorázové kódy pro přihlášení nebo podpis transakcí v aplikaci Online Banking v režimu offline (bez připojení mobilního zařízení k internetu).	V
Hardwarový bezpečnostní klíč (HW token)	Hardwarové zařízení generující kódy chráněné PINem. Používá se pro generování jednorázových číselných kódů pro přihlašování nebo autorizaci platebních příkazů.	V
Registrované mobilní telefonní číslo	Telefonní číslo přiřazené uživateli v UniCredit Bank, které umožňuje přijímat jednorázové bezpečnostní kódy, tzv. SMS OTP (OTP znamená One-Time Password neboli jednorázové heslo).	V
Registrovaná e-mailová adresa	E-mailová adresa přiřazená uživateli v UniCredit Bank. E-mailová adresa umožňuje přijímat jednorázové bezpečnostní kódy (e-mail OTP).	V
Otisk prstu (biometrie)	Otisk prstu uložený v mobilním zařízení, ve kterém je aktivovaná mobilní aplikace Smart Banking. Používá se pro potvrzení přihlášení nebo autorizaci transakce v aktivované mobilní aplikaci (SW bezpečnostním klíči).	I

Sken tváře (biometrie)	Sken tváře uložený v mobilním zařízení, ve kterém je aktivovaná mobilní aplikace Smart Banking. Používá se pro potvrzení přihlášení nebo autorizaci transakce v aktivované mobilní aplikaci (SW bezpečnostním klíči). Sken tváře se porovnává s biometrickými údaji uloženými u nás nebo vůči Vaší fotografii (např. z identifikačního dokladu). Používá se např. při silném ověření klienta při aktivaci mobilní aplikace (SW bezpečnostního klíče).	I
Heslo pro komunikaci s bankou	Heslo, skládající se z různých alfanumerických znaků (délka 6–14 znaků). Toto heslo se používá pro ověření uživatele při telefonickém kontaktu s UniCredit Bank.	Z
Jednorázové bezpečnostní heslo (OTP = One-Time Password)	Jednorázový bezpečnostní kód, pomocí něhož lze ověřit vlastnictví bezpečnostního prvku. Je to kód zasílaný na registrované mobilní telefonní číslo, na registrovanou e-mailovou adresu nebo je generovaný mobilní aplikací SmartBanking. Tento bezpečnostní kód **nikdy nepřeposílejte ani nesdělujte třetím osobám**. Tento kód se používá při aktivaci mobilního bankovnictví, při přihlašování do internetového bankovnictví (při použití metody SMS OTP), při ověření nového telefonního čísla, při resetu PINu apod.	V

Další prvky sloužící pro ověření:

Prvek	Popis
Uživatelské jméno	Uživatelské jméno (přidělené číslo nebo zvolený alias), které se používá pro přihlášení do internetového bankovnictví.
Osobní doklady	Osobní doklady uživatele (občanský průkaz, řidičský průkaz, cestovní pas).
Rodné číslo	Rodné číslo přidělené uživateli.
Kontrolní otázky	Otázky týkající se klienta nebo jeho produktů.
Kód CVV2/CVC2	Speciální trojmístné číslo, které je uvedeno na platební kartě. Je to bezpečnostní prvek používaný k identifikaci držitele karty v prostředí bez přítomnosti platební karty (např. internet).
Číslo platební karty	Unikátní 16místné číslo platební karty.

2. Pravidla pro prvky: PIN/Heslo

a) Nepoužívejte stejná hesla a PINy jako v jiných aplikacích a na internetu (např. v e-shopech, sociálních sítích, e-mailech apod.). Nastavte si bezpečnostní prvek (heslo, PIN), aby nebyl jednoduše uhodnutelný nebo odvoditelný (např. od data narození, od uživatelského jména). Používejte tzv. silná hesla – čím delší a složitější heslo, tím vyšší bezpečnost (např. kombinace malých a velkých písmen, číslic, speciálních znaků apod.).
b) Nikomu nesdělujte ani nikam na internetu nezadávejte své bezpečnostní prvky, nejde-li o aplikace Online Banking a Smart Banking UniCredit Bank. PIN do mobilního bankovnictví zadávejte pouze do aplikace Smart Banking (při aktivaci, při přihlášení, při potvrzení transakce). Heslo (Online Banking) zadávejte pouze do internetového bankovnictví na stránce https://cz.unicreditbanking.eu. Nikdy nezadávejte PIN pro mobilní aplikaci do internetové stránky ani ho nikomu nesdělujte. Tento PIN nikdy nepotřebuje pracovník Policie ČR, České národní banky ani UniCredit Bank. PIN pro mobilní aplikaci je jeden z nejdůležitějších bezpečnostních prvků, který musíte chránit.
c) Hesla a PINy si nepoznamenávejte ve snadno čitelné podobě (např. zapsáním na papír, do nešifrovaného souboru v počítači) a chraňte je před vyzrazením.
d) V případě, že došlo k vyzrazení hesla nebo PIN nebo máte pouhé podezření, že došlo k jejich vyzrazení, heslo nebo PIN neprodleně změňte.
e) Při zadávání bezpečnostních prvků na veřejnosti (např. ve vozidlech hromadné dopravy) nebo v monitorovaných místnostech (např. v blízkosti bezpečnostních kamer) dbejte zvýšené opatrnosti. Ujistěte se, že Vámi zadané údaje nemohou zpozorovat jiné osoby.
f) Nezadávejte své bezpečnostní prvky na počítačích (např. při přihlašování do bankovnictví), kde si nemůžete být jisti, že na nich nejsou nainstalovány škodlivé programy (např. ve veřejných internetových kavárnách, počítačích sdílených více lidmi).
g) Heslo pro komunikaci s bankou sdělte pouze pracovníkovi Unicredit Bank v situaci, kdy je toto heslo vyžadováno. Toto heslo či jeho část vyplňujte pouze do vybraných zaheslovaných dokumentů zaslaných Bankou. Heslo pro komunikaci s bankou sdělte pouze pracovníkovi Unicredit Bank v situaci, kdy je toto heslo vyžadováno.

3. Pravidla pro prvky: aktivovaná mobilní aplikace, hardwarový bezpečnostní klíč, registrované mobilní telefonní číslo, registrovaná e-mailová adresa, jednorázové bezpečnostní heslo

a) Tyto prvky je nutné chránit před neoprávněným přístupem třetí osoby. Odblokování a použití SIM karty chraňte PINem. Pokud dojde ke ztrátě nebo odcizení mobilního zařízení, nebude mít třetí osoba možnost přijímat Vaše bezpečnostní kódy (OTP). I tak SIM kartu nechte co nejdříve zablokovat u operátora.
b) Chraňte svůj profil u mobilního operátora. Nikdy neumožněte, aby si třetí osoba mohla nechat vystavit novou SIM/eSIM k Vašemu telefonnímu číslu.
c) Neumožňujte přístup k svému e-mailovému účtu dalším osobám a nastavte si dvoufaktorové/dvoufázové ověření).
d) Neumožněte přístup do svého mobilního zařízení dalším osobám (např. otiskem prstu, skenem tváře, heslem, PINem), případně nainstalovat do mobilního zařízení škodlivý software.
e) Pokud došlo ke ztrátě nebo odcizení mobilního telefonu (nebo SIM karty) a třetí osoba tak může mít přístup k Vašim SMS zprávám a může provádět hovory z Vašeho telefonního čísla, neprodleně kontaktujte UniCredit Bank a internetové bankovnictví nechte preventivně zablokovat.

UniCredit Bank

4. Pravidla pro prvky: otisk prstu / sken tváře

a) Aplikace Smart Banking může využívat biometrické údaje (otisk prstu, sken tváře) uložené ve Vašem mobilním zařízení. O povolení používání biometrických údajů pro ověření uživatele rozhodujete pouze Vy při aktivaci nebo v nastavení aplikace Smart Banking. Nikdy neumožněte registraci biometrických údajů jiné osoby (ani členů rodiny) do Vašeho mobilního zařízení.

5. Pravidla pro mobilní zařízení používaná pro přístup do aplikace Smart Banking

a) Přístup do mobilního zařízení zabezpečte přístupovým heslem, PINem nebo biometricky (otisk prstu, sken tváře). Nenechávejte své mobilní zařízení bez dozoru a používejte automatické zamykání zařízení (obrazovky) po krátké době.
b) Nepoužívejte programové úpravy mobilního zařízení, které umožňují plný administrátorský přístup do něj (např. jailbreak, root).
c) Pravidelně aktualizujte operační systém svého mobilního zařízení i jednotlivých instalovaných aplikací.
d) Na svém mobilním zařízení používejte nejnovější verzi bezpečnostních programů (např. antivir, firewall), které pravidelně aktualizujte.
e) V nově instalované nebo aktualizované aplikaci v mobilním zařízení nepovolujte nadbytečná oprávnění (např. přístup k SMS, usnadnění, nastavení apod.). Škodlivá aplikace se širokými oprávněními Vás může sledovat včetně zadávaných bezpečnostních prvků a odesílat je třetí straně (útočníkovi).
f) Do mobilních zařízení instalujte pouze aplikace z oficiálních obchodů s aplikacemi – Google Play (Android), App Store (iOS) včetně případných doplňků, které Vás používaná aplikace vyzývá doinstalovat. Ve svém mobilním zařízení si nastavte zákaz instalace aplikací z neznámých zdrojů.
g) Neinstalujte aplikace na základě pokynů cizí osoby a zejména cizím osobám nepovolujte vzdálený přístup do mobilního telefonu (např. přes aplikaci AnyDesk).

6. Pravidla pro zařízení používané pro přístup do aplikace Online Banking

a) Nepřihlašujte se do internetového bankovnictví na zařízení, když si nemůžete být jisti, že na nich nejsou nainstalovány škodlivé programy (např. ve veřejných internetových kavárnách, počítačích sdílených více lidmi). Pokud máte o bezpečnosti zařízení pochybnosti, nepoužívejte ho. Ideálně se přihlašujte ze zařízení, které máte plně pod svojí kontrolou, např. z domácího počítače.
b) Nepřihlašujte se na počítač jako administrátor, pokud to není nutné. Přihlašujte se na počítač jako běžný uživatel.
c) Pravidelně aktualizujte operační systém a své programy, zejména internetový prohlížeč.
d) Rozšíření (plug-iny) prohlížeče instalujte v omezené míře a pouze od známých a důvěryhodných vydavatelů.
e) Používejte nejnovější verzi bezpečnostních programů (např. antivir, firewall), které pravidelně aktualizujte.
f) Chraňte počítač před neoprávněným přístupem dalších osob nastavením přístupových oprávnění, zabezpečením heslem, případně dalšími prvky.
g) Nepovolujte cizím osobám vzdálený přístup do počítače (např. přes aplikaci AnyDesk).

7. Další pravidla, jejichž dodržování zvýší pravděpodobnost, že nepřijdete o finanční prostředky

a) Přístup do internetového bankovnictví
   (i) Adresu webové stránky UniCredit Bank zadávejte ručně. Pro přístup na stránky aplikace Online Banking využijte www.unicreditbank.cz, odkud přejděte na přihlašovací stránku internetového bankovnictví. Zkontrolujte, že přistupujete na webovou adresu https://cz.unicreditbanking.eu. Nepoužívejte zástupce na přihlašovací stránku internetového bankovnictví.
   (ii) Nikdy nepřistupujte do internetového bankovnictví přes odkaz z vyhledávače ani odkaz zaslaný e-mailem, SMS nebo jiným způsobem (na sociální síti, přes chatovací aplikaci atd.).
   (iii) Pokud se Vám přihlašovací obrazovka k produktům internetového bankovnictví zdá jakkoli podezřelá, nepřihlašujte se, protože útočníci dokážou velmi věrně napodobit vzhled přihlašovací stránky a nenápadně Vás na ni navést, např. přes SMS, e-mail apod.

b) Ověřování totožnosti uživatele prostřednictvím BankiD
   (i) Dávejte pozor, na jakých stránkách se chystáte bankovní identitu použít.
   (ii) Kontrolujte, jaké údaje a komu v rámci BankiD poskytujete.
   (iii) Při používání bankovní identity se ujistěte, že své bezpečnostní prvky zadáváte skutečně na stránkách UniCredit Bank (https://cz.unicreditbanking.eu).
   (iv) Dodržujte stejná pravidla jako u internetového nebo mobilního bankovnictví.

c) Kontrolujte, co potvrzujete
   (i) Před potvrzením přihlášení nebo před autorizací platební transakce vždy zkontrolujte, že zadané údaje (např. částka, příjemce) odpovídají Vašemu záměru.
   (ii) Pokud Vám někdo chce poslat peníze, jeho akci není třeba nijak potvrzovat. Na zaslané odkazy neklikejte a ani na výzvu jiné osoby nikdy nezadávejte Vaše bezpečnostní prvky do žádné aplikace.

d) Sledujte aktivitu na Vašem účtu
   (i) Vědět, jaké platby proběhly na Vašich účtech, je nejlepší nástroj včasného varování, že je cokoliv v nepořádku. Nechte si proto automaticky posílat SMS, e-maily či oznámení do mobilního telefonu (tzv. push-notifikace) s informacemi o uskutečněných transakcích.
   (ii) V případě, že na účtu proběhne aktivita s vyšší mírou rizika (např. aktivace mobilního bankovnictví, změna kontaktních údajů apod.), informujeme Vás příslušnou zprávou (např. push-notifikace, e-mail, SMS).
   (iii) Pokud zaregistrujete operaci, kterou jste neprovedli, okamžitě nás kontaktujte na Infolinku UniCredit Bank.

UniCredit Bank

e) Nikdy nereagujte na telefonáty, které Vás vybízejí k akci s účtem
   (i) Pravděpodobně se jedná o falešného bankéře, falešného policistu či falešného pracovníka státní instituce (ČNB, NÚKIB apod.). UniCredit Bank nikdy telefonicky nevyzývá své klienty k jakýmkoliv transakcím, ať už se jedná o výběr z účtu, platební transakci či dokonce žádost o úvěr.

f) S podezřelými zprávami zacházejte opatrně
   (i) U každého e-mailu a SMS zprávy zkontrolujte adresu skutečného odesílatele a případný webový odkaz, na který Vás e-mail/SMS vybízí kliknout.
   (ii) Rizikové mohou být také zprávy v nejrůznějších chatovacích aplikacích (WhatsApp, Messenger apod.) obsahující aktivní odkaz. E-maily od nás Vám mohou přijít pouze z domény: unicreditbank.cz nebo unicreditgroup.cz. Pokud e-mail z UniCredit Bank dorazí z jiné domény, neotvírejte ho.
   (iii) UniCredit Bank nikdy neposílá e-maily či jiné zprávy vyzývající Vás ke sdělení bezpečnostních prvků. Na podobné zprávy nikdy nereagujte a informujte nás prostřednictvím Infolinky UniCredit Bank.
   (iv) Pokud se zpráva od UniCredit Bank jeví jakkoliv podezřele a nejste si jisti, kontaktujte nás na naší Infolince. Pokud jste již zprávu otevřeli, určitě neotevírejte přílohy nestandardního typu souboru (např. přípony: .exe, .php) a neklikejte na odkazy obsažené ve zprávě. Pokud by se Vám to nedopatřením stalo, rychle vše zavřete a nenechávejte program ani prohlížeč nic instalovat. Spusťte antivirovou kontrolu a ozvěte se nám.
   (v) Ve své e-mailové schránce používejte ochranu proti nevyžádané poště (spam, phishing).

g) Pravidelně sledujte novinky o bezpečnosti na internetu
   (i) Čím více informací máte, tím bezpečněji se dokážete na internetu chovat. Pravidelně proto sledujte nejnovější zprávy z oblasti bezpečnosti na internetu a dodržujte všechny doporučené zásady.

h) Čtěte zasílané zprávy
   (i) E-maily, dopisy a další zprávy nejsou vždycky zábavné. Zato často bývají důležité a vyplatí se je číst pozorně. Platí to i pro zprávy zasílané do mobilního telefonu.

i) Reagujte včas. Ihned kontaktujte Infolinku UniCredit Bank
   (i) Reagujte na případné bezpečnostní upozornění, které můžete obdržet, pokud nastane riziková událost. V případě podezření na podvod nebo bezpečnostní hrozbu UniCredit Bank klienty vhodným způsobem informuje, a to s využitím primárních kontaktních údajů, které klienti uvedli při uzavírání smlouvy.

8. Autorizace (podpis) aktivní operace / platební transakce a odvolání platební transakce

UniCredit Bank umožňuje klientům/uživatelům podepsat různé druhy aktivních operací – např. platební příkaz, smlouvu, dokument či jiný úkon. Způsob autorizace v jednotlivých aplikacích se liší a je následující:

Autorizace v aplikaci Smart Banking

a) Podpis biometricky – podpis otiskem prstu či skenem obličeje.
   V tomto případě je uživatel vyzván k použití otisku prstu či skenu obličeje.
b) Podpis zadáním PINu – podpis operace zadáním PINu. V tomto případě je uživatel vyzván k použití PINu.

Autorizace v aplikaci Online Banking

a) Smart klíč
   (i) Online metoda – na mobilní telefon do aplikace Smart Banking obdržíte oznámení (push-notifikace). Po otevření zprávy zkontrolujete detaily operace k podpisu a podepíšete ji biometricky či zadáním PINu.
   (ii) Offline metoda – aplikace Online Banking Vám zobrazí QR kód, který ofotíte aplikací Smart Banking (její část „Smart klíč"), která vygeneruje 6místný jednorázový kód, a ten přepíšete do aplikace Online Banking a potvrdíte.

b) SMS klíč
Tato metoda se skládá z kombinace osobního hesla a jednorázových kódů zaslaných na Váš mobilní telefon. Uživatel zadá své statické heslo. V případě zadání správného hesla odešle UniCredit Bank uživateli SMS zprávu na uživatelem určený mobilní telefon formou SMS obsahující OTP. Tento časově omezený kód uživatel přepíše zpět do Online Bankingu, a potvrdí tak tím operaci.

c) Hardwarový token
Heslo pro podpis operace je vygenerován tokenem (tzv. „kalkulačky"). Přístup do bezpečnostního klíče je chráněn PIN kódem, který si volí uživatel. Uživatel zadá PIN přímo na klávesnici tokenu.
V případě zadání správného PIN token vygeneruje 8místný jednorázový kód, který uživatel přepíše do aplikace Online Banking. Aplikace poté zobrazí 6místný jednorázový kód (OTP), který uživatel přepíše opět do aplikace Online Banking. Pokud je OTP správný, operace je úspěšně podepsána.

d) Odvolání platební transakce
Odvolání platební transakce se uskuteční stejným způsobem jako její autorizace, pokud odvolání příslušná aplikace připouští.

9. Odpovědnost za ztrátu finančních prostředků v případě ztráty, odcizení, zneužití nebo neoprávněného použití platebního prostředku nebo osobního bezpečnostního prvku

a) Neautorizovanou nebo nesprávně provedenou platební transakci, ztrátu, odcizení, zneužití nebo neoprávněné použití Vašeho platebního prostředku nebo osobního bezpečnostního prvku, osobních dokladů, mobilního telefonu s uloženou platební kartou, s aktivovaným mobilním bankovnictvím nebo cokoliv podezřelého v souvislosti s internetovým nebo mobilním bankovnictvím nám neprodleně, nejpozději však do 10 pracovních dní, nahlašte na Infolinku UniCredit Bank: +420 221 210 031 (24/7, non stop) nebo na kterékoli naší pobočce v rámci otevírací doby.

b) Ztrátu finančních prostředků vzniklou z neautorizované platební transakce nesete do částky odpovídající 50 eurům, byla-li tato ztráta způsobena použitím ztraceného nebo odcizeného platebního prostředku nebo osobního bezpečnostního prvku nebo zneužitím platebního prostředku nebo osobního bezpečnostního prvku, pokud jsou současně splněny následující podmínky:

   (i) K provedení Vámi neuatorizované platební transakce došlo poté, co jste nahlásil(a) UniCredit Bank ztrátu, odcizení, zneužití nebo neoprávněné použití platebního prostředku nebo osobního bezpečnostního prvku.
   (ii) Úmyslně nebo hrubě nedbale jste neporušil(a) povinnost chránit osobní bezpečnostní prvky.

c) Ztrátu finančních prostředků vzniklou z neautorizované platební transakce nesete v plném rozsahu, jestliže jste způsobil(a) tuto ztrátu svým podvodným jednáním nebo tím, že jste úmyslně nebo hrubě nedbale porušil(a) povinnost chránit osobní bezpečnostní prvky. Za úmyslné porušení povinnosti chránit osobní bezpečnostní prvky nebo za porušení povinnosti chránit osobní bezpečnostní prvky v důsledku hrubé nedbalosti je považováno nedodržení pravidel uvedených v tomto dokumentu jakož i ve všeobecně závazných právních předpisech.

10. Odpovědnost za nesprávně provedenou platební transakci

O nesprávně provedenou platební transakci se jedná, jestliže UniCredit Banka nezúčtovala částku platební transakce ve správné měně nebo nepoužila číslo účtu nebo jiný jedinečný identifikátor v souladu s Vaším příkazem.

Jestliže má UniCredit Bank povinnost napravit nesprávně provedenou platební transakci a Vy jí oznámíte, že netrváte na provedení platební transakce, UniCredit Bank neprodleně:

a) uvede Váš účet do stavu, v němž by byl, kdyby k tomuto odepsání nedošlo, nebo
b) vrátí na Váš účet částku, jakož i poplatek za převod částky a ušlé úroky, jestliže postup podle písmene a) nepřipadá v úvahu.

Jestliže neoznámíte UniCredit Bank, že netrváte na provedení platební transakce, UniCredit Bank neprodleně:
a) zajistí připsání částky nesprávně provedené platební transakce na účet banky příjemce, a
b) uvede Váš účet do stavu, v němž by byl, kdyby UniCredit Bank provedla platební transakci správně, nebo
c) vrátí Vám nesprávně zaplacený poplatek a ušlé úroky, jestliže postup podle písmene a) nepřipadá v úvahu.