Pravidlá bezpečného používania internetového bankovníctva

Účinnosť od 2. 9. 2024

Účelom tohto dokumentu je poskytnúť Vám pred uzatvorením rámcovej zmluvy a predovšetkým zmluvy umožňujúcej využívať služby internetového bankovníctva informácie podľa zákona č. 492/2009 Z.z. o platobných službách.

Poskytovateľom služieb internetového bankovníctva je UniCredit Bank Czech Republic and Slovakia, a.s., so sídlom Želetavská 1525/1, 140 92 Praha 4 – Michle, zapísaná v obchodnom registri vedenom Mestským súdom v Prahe, oddiel B, vložka 3608, IČO 64948242 pri vykonávaní bankových činností na území Slovenskej republiky prostredníctvom UniCredit Bank Czech Republic and Slovakia, a.s., pobočka zahraničnej banky, Šancová 1/A, 813 33 Bratislava, IČO: 47 251 336, zapísaná v obchodnom registri Mestského súdu Bratislava III, oddiel: Po, vložka číslo: 2310/B; Banka poskytuje svoje služby v Slovenskej republike na základe jedného bankového povolenia podľa práva Európskej únie, oznámením Českej národnej banky č. 2013/5785/570 zo dňa 20. mája 2013 a oznámením podmienok pôsobenia pobočky zahraničnej banky na území Slovenskej republiky na základe jedného bankového povolenia Národnej banky Slovenska č. OBD-5659/2013 zo dňa 4. júla 2013.

Ako klient/používateľ môžete v rámci internetového bankovníctva v aplikácii Smart Banking alebo Online Banking prostredníctvom siete internet využívať určité bankové služby, komunikovať s UniCredit Bank dohodnutým spôsobom a najmä autorizovať príslušné platobné transakcie alebo iné pokyny. Každé Vaše potvrdenie, súhlas alebo iné konanie obdobnej povahy uskutočnené v internetovom bankovníctve s použitím príslušného osobného bezpečnostného prvku sa považuje za Váš záväzný prejav vôle.

1. Osobné bezpečnostné prvky slúžiace na overenie používateľa (ďalej len „bezpečnostné prvky“)

Prvky slúžiace na Vaše overenie sú jedinečné bezpečnostné prvky, ktoré Vám umožňujú vstupovať do internetového bankovníctva a využívať produkty aplikácií Smart Banking alebo Online Banking. Tieto prvky sme Vám buď pridelili alebo ste si ich sami vybrali. Každý prvok je určitého typu:

a) Znalosť (Z) – tzn. niečo, čo pozná len používateľ;
b) Vlastníctvo (V) – tzn. niečo, čo má len používateľ;
c) Inherencia/Biometria (I) – niečo, čím je používateľ (unikátny údaj o používateľovi).

Ak sú na overenie použité minimálne 2 prvky, každý musí byť z inej kategórie, ide o tzv. „silné overenie klienta“.

Osobné bezpečnostné prvky sú:

Prvok	Opis	Typ
PIN pre mobilnú aplikáciu	Číselný kód pre mobilnú aplikáciu Smart Banking, ktorý sa používa pri aktivácii, prihlásení alebo na potvrdzovanie transakcií. Tento PIN je neprenosný, nastavuje si ho sám používateľ a **môže ho poznať len používateľ** (podobne ako PIN k platobnej karte). Tento PIN sa používa len v aplikácii Smart Banking.	Z
Heslo	Heslo sa skladá z numerických znakov (dĺžka 6 znakov). Používa sa na prihlásenie do internetového bankovníctva Online Banking (v kombinácii s jednorazovým SMS kódom). Heslo je neprenosné a môže ho poznať len používateľ. Úvodné heslo si musí používateľ ihneď zmeniť na svoje. Heslo sa používa len v aplikácii Online Banking (na adrese sk.unicreditbanking.eu).	Z
Aktivovaná mobilná aplikácia (SW bezpečnostný kľúč)	Mobilná aplikácia Smart Banking v sebe obsahuje „bezpečnostný kľúč“ (Smart kľúč). Po aktivácii je aplikácia jednoznačne spojená s používateľom. Aplikácia umožňuje prijímať push notifikačné správy, pomocou ktorých možno potvrdiť prihlásenie do aplikácie Online Banking alebo autorizovať platobnú transakciu. Aplikácia umožňuje generovať jednorazové kódy na prihlásenie alebo autorizáciu transakcií v aplikácii Online Banking v režime offline (bez pripojenia mobilného zariadenia k internetu).	V
Hardvérový bezpečnostný kľúč (HW token)	Hardvérové zariadenie generujúce kód chránené PIN kódom. Používa sa na generovanie jednorazových číselných kódov na prihlasovanie alebo autorizáciu platobných príkazov.	V
Registrované mobilné telefónne číslo	Telefónne číslo priradené používateľovi v UniCredit Bank, ktoré umožňuje prijímať jednorazové bezpečnostné kódy, tzv. SMS OTP (OTP znamená One-Time Password alebo jednorazové heslo).	V
Registrovaná e-mailová adresa	E-mailová adresa priradená používateľovi v UniCredit Bank. E-mailová adresa umožňuje prijímať jednorazové bezpečnostné kódy (e-mail OTP).	V
Odtlačok prsta (biometria)	Odtlačok prsta uložený v mobilnom zariadení, v ktorom je aktivovaná mobilná aplikácia Smart Banking. Používa sa na potvrdenie prihlásenia alebo autorizáciu transakcie v aktivovanej mobilnej aplikácii (SW bezpečnostnom kľúči).	I

Sken tváre (biometria)	Sken tváre uložený v mobilnom zariadení, v ktorom je aktivovaná mobilná aplikácia Smart Banking. Používa sa na potvrdenie prihlásenia alebo autorizáciu transakcie v aktivovanej mobilnej aplikácii (SW bezpečnostnom kľúči). Sken tváre sa porovnáva s biometrickými údajmi uloženými v UniCredit Bank alebo s Vašou fotografiou (napr. z identifikačného dokladu). Používa sa napr. pri silnom overení klienta pri aktivácii mobilnej aplikácie (SW bezpečnostného kľúča).	I
Heslo na komunikáciu s bankou	Heslo skladajúce sa z rôznych alfanumerických znakov (dĺžka 6 – 14 znakov). Toto heslo sa používa na overenie používateľa pri telefonickom kontakte s UniCredit Bank.	Z
Jednorazové bezpečnostné heslo (OTP = One-Time Password)	Jednorazový bezpečnostný kód, pomocou ktorého možno overiť vlastníctvo bezpečnostného prvku. Je to kód zasielaný na registrované mobilné telefónne číslo, na registrovanú e-mailovú adresu alebo je generovaný mobilnou aplikáciou Smart Banking. Tento bezpečnostný kód **nikdy neprepošielajte ani neposkytujte tretím osobám**. Tento kód sa používa pri aktivácii mobilného bankovníctva, pri prihlasovaní do internetového bankovníctva (pri použití metódy SMS OTP), pri overení nového telefónneho čísla, pri resete PIN kódu a pod.	V

Ďalšie prvky slúžiace na overenie:

Prvok	Opis
Používateľské meno	Používateľské meno (pridelené číslo alebo vybraný alias), ktoré sa používa na prihlásenie do internetového bankovníctva.
Osobné doklady	Osobné doklady používateľa (občiansky preukaz, vodičský preukaz, cestovný pas).
Rodné číslo	Rodné číslo pridelené používateľovi.
Kontrolné otázky	Otázky týkajúce sa klienta alebo jeho produktov.
Kód CVV2/CVC2	Špeciálne trojmiestne číslo, ktoré je uvedené na platobnej karte. Je to bezpečnostný prvok používaný na identifikáciu držiteľa karty v prostredí bez prítomnosti platobnej karty (napr. internet).
Číslo platobnej karty	Unikátne 16-miestne číslo platobnej karty.

2. Pravidlá pre prvky: PIN/Heslo

a) Nepoužívajte rovnaké heslá a PIN kódy ako v iných aplikáciách a na internete (napr. v e-shopoch, sociálnych sieťach, e-mailoch a pod.). Nastavte si bezpečnostný prvok (heslo, PIN), aby nebol jednoducho uhádnuteľný alebo odvoditeľný (napr. od dátumu narodenia, od používateľského mena). Používajte tzv. silné heslá – čím dlhšie a zložitejšie heslo, tým vyššia bezpečnosť (napr. kombinácia malých a veľkých písmen, číslic, špeciálnych znakov a pod.).
b) Nikomu neposkytujte ani nikam na internete nezadávajte svoje bezpečnostné prvky, ak nejde o aplikácie Online Banking a Smart Banking UniCredit Bank. PIN do mobilného bankovníctva zadávajte len do aplikácie Smart Banking (pri aktivácii, pri prihlásení, pri potvrdení transakcie). Heslo (Online Banking) zadávajte len do internetového bankovníctva na stránke https://sk.unicreditbanking.eu. Nikdy nezadávajte PIN pre mobilnú aplikáciu na internetovej stránke ani ho nikomu neposkytujte. Tento PIN nikdy nepotrebuje pracovník Polície SR, Národnej banky Slovenska ani UniCredit Bank. PIN pre mobilnú aplikáciu je jeden z najdôležitejších bezpečnostných prvkov, ktorý musíte chrániť.
c) Heslá a PIN kódy si nepoznamenávajte v jednoducho čitateľnej podobe (napr. zapísaním na papier, do nešifrovaného súboru v počítači) a chráňte ich pred vyzradením.
d) V prípade, že heslo alebo PIN boli vyzradené alebo máte len podozrenie, že boli vyzradené, heslo alebo PIN bezodkladne zmeňte.
e) Pri zadávaní bezpečnostných prvkov na verejnosti (napr. vo vozidlách hromadnej dopravy) alebo v monitorovaných miestnostiach (napr. v blízkosti bezpečnostných kamier) dbajte na zvýšenú opatrnosť. Ubezpečte sa, že Vami zadané údaje nemôžu spozorovať iné osoby.
f) Nezadávajte svoje bezpečnostné prvky na počítačoch (napr. pri prihlasovaní do bankovníctva), kde si nemôžete byť istý, že na nich nie sú nainštalované škodlivé programy (napr. vo verejných internetových kaviarňach, počítačoch zdieľaných viacerými ľuďmi).
g) Heslo na komunikáciu s bankou poskytnite len pracovníkovi UniCredit Bank v situácii, kedy sa toto heslo vyžaduje. Toto heslo alebo jeho časť zadajte len do vybraných zaheslovaných dokumentov zaslaných Bankou.

3. Pravidlá pre prvky: aktivovaná mobilná aplikácia, hardvérový bezpečnostný kľúč, registrované mobilné telefónne číslo, registrovaná e-mailová adresa, jednorazové bezpečnostné heslo

a) Tieto prvky treba chrániť pred neoprávneným prístupom tretej osoby. Odblokovanie a použitie SIM karty chráňte PIN kódom. Ak sa mobilné zariadenie stratí alebo je odcudzené, nebude mať tretia osoba možnosť prijímať Vaše bezpečnostné kódy (OTP). Aj tak SIM kartu nechajte čo najskôr zablokovať u operátora.
b) Chráňte svoj profil u mobilného operátora. Nikdy neumožnite, aby si tretia osoba mohla nechať vystaviť novú SIM/eSIM k Vášmu telefónnemu číslu.
c) Neumožňujte prístup k svojmu e-mailovému účtu ďalším osobám a nastavte si dvojfaktorové/dvojfázové overenie).
d) Neumožnite prístup do svojho mobilného zariadenia ďalším osobám (napr. odtlačkom prsta, skenom tváre, heslom, PIN kódom), prípadne nainštalovať do mobilného zariadenia škodlivý softvér.
e) Ak sa mobilný telefón (alebo SIM karta) stratil alebo bol odcudzený a tretia osoba tak môže mať prístup k Vašim SMS správam a môže uskutočňovať hovory z Vášho telefónneho čísla, bezodkladne kontaktujte UniCredit Bank a internetové bankovníctvo nechajte preventívne zablokovať.

UniCredit Bank

4. Pravidlá pre prvky: odtlačok prsta / sken tváre

a) Aplikácia Smart Banking môže využívať biometrické údaje (odtlačok prsta, sken tváre) uložené vo Vašom mobilnom zariadení. O povolení používania biometrických údajov na overenie používateľa rozhodujete len Vy pri aktivácii alebo v nastavení aplikácie Smart Banking. Nikdy neumožnite registráciu biometrických údajov inej osoby (ani členov rodiny) do Vášho mobilného zariadenia.

5. Pravidlá pre mobilné zariadenia používané na prístup do aplikácie Smart Banking

a) Prístup do mobilného zariadenia zabezpečte prístupovým heslom, PIN kódom alebo biometricky (odtlačok prsta, sken tváre). Nenechávajte svoje mobilné zariadenie bez dozoru a používajte automatické zamykanie zariadenia (obrazovky) po krátkom čase.
b) Nepoužívajte programové úpravy mobilného zariadenia, ktoré umožňujú plný administrátorský prístup do nej (napr. jailbreak, root).
c) Pravidelne aktualizujte operačný systém svojho mobilného zariadenia aj jednotlivých inštalovaných aplikácií.
d) Na svojom mobilnom zariadení používajte najnovšiu verziu bezpečnostných programov (napr. antivírus, firewall), ktoré pravidelne aktualizujte.
e) V novoinštalovanej alebo aktualizovanej aplikácii v mobilnom zariadení nepovoľujte nadbytočné oprávnenia (napr. prístup k SMS, zjednodušenie, nastavenia a pod.). Škodlivá aplikácia s rozsiahlymi oprávneniami Vás môže sledovať vrátane zadávaných bezpečnostných prvkov a odosielať ich tretej strane (útočníkovi).
f) Do mobilných zariadení inštalujte len aplikácie z oficiálnych obchodov s aplikáciami – Google Play (Android), App Store (iOS) vrátane prípadných doplnkov, ktoré Vás používaná aplikácia vyzýva doinštalovať. Vo svojom mobilnom zariadení si nastavte zákaz inštalácie aplikácií z neznámych zdrojov.
g) Neinštalujte aplikácie na základe pokynov cudzej osoby a najmä cudzím osobám nepovoľujte vzdialený prístup do mobilného telefónu (napr. cez aplikáciu AnyDesk).

6. Pravidlá pre zariadenia používané na prístup do aplikácie Online Banking

a) Neprihlasujte sa do internetového bankovníctva na zariadení, ak si nemôžete byť istý, že na nich nie sú nainštalované škodlivé programy (napr. vo verejných internetových kaviarňach, počítačoch zdieľaných viacerými ľuďmi). Ak máte o bezpečnosti zariadenia pochybnosti, nepoužívajte ho. Ideálne sa prihlasujte zo zariadení, ktoré máte plne pod svojou kontrolou, napr. z domáceho počítača.
b) Neprihlasujte sa na počítač ako administrátor, ak to nie je nutné. Prihlasujte sa na počítač ako bežný používateľ.
c) Pravidelne aktualizujte operačný systém a svoje programy, najmä internetový prehliadač.
d) Rozšírenia (plug-iny) prehliadača inštalujte v obmedzenej miere a len od známych a dôveryhodných vydavateľov.
e) Používajte najnovšiu verziu bezpečnostných programov (napr. antivírus, firewall), ktoré pravidelne aktualizujte.
f) Chráňte počítač pred neoprávneným prístupom ďalších osôb nastavením prístupových oprávnení, zabezpečením heslom, prípadne ďalšími prvkami.
g) Nepovoľujte cudzím osobám vzdialený prístup do počítača (napr. cez aplikáciu AnyDesk).

7. Ďalšie pravidlá, ktorých dodržiavanie zvýši pravdepodobnosť, že neprídete o finančné prostriedky

a) Prístup do internetového bankovníctva
   (i) Adresu webovej stránky UniCredit Bank zadávajte ručne. Na prístup na stránky aplikácie Online Banking využite www.unicreditbank.sk, odkiaľ prejdete na prihlasovaciu stránku internetového bankovníctva. Skontrolujte, že pristupujete na webovú adresu https://sk.unicreditbanking.eu. Nepoužívajte zástupcu na prihlasovaciu stránku internetového bankovníctva.
   (ii) Nikdy nepristupujte do internetového bankovníctva cez odkaz z vyhľadávača ani odkaz zaslaný e-mailom, SMS alebo iným spôsobom (na sociálnej sieti, cez chatovaciu aplikáciu atď.).
   (iii) Ak sa Vám prihlasovacia obrazovka k produktom internetového bankovníctva zdá akokoľvek podozrivá, neprihlasujte sa, pretože útočníci dokážu veľmi verne napodobniť vzhľad prihlasovacej stránky a nenápadne Vás na ňu naviesť, napr. cez SMS, e-mail a pod.

b) Kontrolujte, čo potvrdzujete
   (i) Pred potvrdením prihlásenia alebo pred autorizáciou platobnej transakcie vždy skontrolujte, že zadané údaje (napr. suma, príjemca) zodpovedajú Vášmu zámeru.
   (ii) Ak Vám chce niekto poslať peniaze, jeho akciu netreba nijako potvrdzovať. Na zaslané odkazy neklikajte a ani na výzvu inej osoby nikdy nezadávajte Vaše bezpečnostné prvky do žiadnej aplikácie.

c) Sledujte aktivitu na Vašom účte
   (i) Vedieť, aké platby sa uskutočnili na Vašich účtoch, je najlepší nástroj včasného varovania, že niečo nie je v poriadku. Nechajte si preto automaticky posielať SMS, e-maily alebo oznámenia do mobilného telefónu (tzv. push notifikácie) s informáciami o uskutočnených transakciách.
   (ii) V prípade, že na účte sa uskutoční aktivita s vyššou mierou rizika (napr. aktivácia mobilného bankovníctva, zmena kontaktných údajov a pod.), informujeme Vás príslušnou správou (napr. push notifikácia, e-mail, SMS).
   (iii) Ak zaregistrujete operáciu, ktorú ste nevykonali, okamžite nás kontaktujte na Infolinku UniCredit Bank.

d) Nikdy nereagujte na telefonáty, ktoré Vás vyzývajú vykonať akciu na účte
   (i) Pravdepodobne ide o falošného bankára, falošného policajta alebo falošného pracovníka štátnej inštitúcie (NBS, NBÚ a pod.). UniCredit Bank nikdy telefonicky nevyzýva svojich klientov na akékoľvek transakcie, či už ide o výber z účtu, platobnú transakciu alebo dokonca žiadosť o úver.

UniCredit Bank

e) S podozrivými správami zaobchádzajte opatrne.
   (i) Pri každom e-maile a SMS správe skontrolujte adresu skutočného odosielateľa a prípadný webový odkaz, na ktorý Vás e-mail/SMS vyzýva kliknúť.
   (ii) Rizikové môžu byť tiež správy v najrôznejších chatovacích aplikáciách (WhatsApp, Messenger a pod.) obsahujúce aktívny odkaz. E-maily od nás Vám môžu prísť len z domény: unicreditbank.sk alebo unicreditgroup.sk. Ak e-mail z UniCredit Bank príde z inej domény, neotvárajte ho.
   (iii) UniCredit Bank nikdy neposiela e-maily ani iné správy vyzývajúce Vás na poskytnutie bezpečnostných prvkov. Na podobné správy nikdy nereagujte a informujte nás prostredníctvom Infolinky UniCredit Bank.
   (iv) Ak sa správa od UniCredit Bank zdá akokoľvek podozrivá a nie ste si istý, kontaktujte nás na našej Infolinke. Ak ste už správu otvorili, určite neotvárajte prílohy neštandardného typu súboru (napr. prípony: .exe, .php). a neklikajte na odkazy obsiahnuté v správe. Ak by sa Vám to nedopatrením stalo, rýchlo všetko zatvorte a nenechávajte program ani prehliadač nič inštalovať. Spustite antivírusovú kontrolu a ozvite sa nám.
   (v) Vo svojej e-mailovej schránke používajte ochranu proti nevyžiadanej pošte (spam, phishing).

f) Pravidelne sledujte novinky o bezpečnosti na internete
   (i) Čím viac informácií máte, tým bezpečnejšie sa dokážete správať na internete. Pravidelne preto sledujte najnovšie správy z oblasti bezpečnosti na internete a dodržiavajte všetky odporúčané zásady.

g) Čítajte zasielané správy
   (i) E-maily, listy a ďalšie správy nie sú vždy zábavné. Avšak často bývajú dôležité a oplatí sa ich pozorne čítať. Platí to aj pre správy zasielané do mobilného telefónu.

h) Váhate? Reagujte včas. Ihneď kontaktujte Infolinku UniCredit Bank
   (i) Reagujte na prípadné bezpečnostné upozornenie, ktoré môžete dostať, ak nastane riziková udalosť. V prípade podozrenia na podvod alebo bezpečnostnú hrozbu UniCredit Bank klienta vhodným spôsobom informuje, a to s využitím primárnych kontaktných údajov, ktoré klient uviedol pri uzatváraní zmluvy.

8. Autorizácia (podpis) aktívnej operácie / platobnej transakcie a odvolanie platobnej transakcie

UniCredit Bank umožňuje klientom/používateľom podpísať rôzne druhy aktívnych operácií – napr. platobný príkaz, zmluvu, dokument alebo iný úkon. Spôsob autorizácie v jednotlivých aplikáciách sa líši a je nasledujúci:

Autorizácia v aplikácii Smart Banking

a) Podpis **biometricky** – podpis odtlačkom prsta alebo skenom tváre.
   V tomto prípade je používateľ vyzvaný použiť odtlačok prsta alebo sken tváre.
b) Podpis zadaním **PIN** – podpis operácie zadaním PIN. V tomto prípade je používateľ vyzvaný použiť PIN.

Autorizácia v aplikácii Online Banking

a) Smart kľúč
   (i) Online metóda – na mobilný telefón do aplikácie Smart Banking dostanete oznámenie (push notifikácia). Po otvorení správy skontrolujete detaily operácie na podpis a podpíšete ju biometricky alebo zadaním PIN.
   (ii) Offline metóda – aplikácia Online Banking Vám zobrazí QR kód, ktorý odfotíte aplikáciou Smart Banking (jej časť „Smart kľúč"), ktorá vygeneruje 6-miestny jednorazový kód, a ten prepíšete do aplikácie Online Banking a potvrdíte.

b) SMS kľúč
Táto metóda sa skladá z kombinácie osobného hesla a jednorazových kódov zaslaných na Váš mobilný telefón.
Používateľ zadá svoje statické heslo. V prípade zadania správneho hesla odošle UniCredit Bank používateľovi SMS správu na používateľom určený mobilný telefón formou SMS obsahujúcej OTP. Tento časovo obmedzený kód používateľ prepíše späť do Online Bankingu a potvrdí tak tým operáciu.

c) Hardvérový token
Heslo na podpis operácie je vygenerované tokenom (tzv. „kalkulačky"). Prístup do bezpečnostného kľúča je chránený PIN kódom, ktorý si volí používateľ. Používateľ zadá PIN priamo na klávesnici tokenu.
V prípade zadania správneho PIN token vygeneruje 8-miestny jednorazový kód, ktorý používateľ prepíše do aplikácie Online Banking. Aplikácia potom zobrazí 6-miestny jednorazový kód (OTP), ktorý používateľ prepíše opäť do aplikácie Online Banking. Ak je OTP správny, operácia je úspešne podpísaná.

d) Odvolanie platobnej transakcie
Odvolanie platobnej transakcie sa uskutoční rovnakým spôsobom, ako jej autorizácia, ak príslušná aplikácia pripúšťa odvolanie.

9. Zodpovednosť za stratu finančných prostriedkov v prípade straty, odcudzenia, zneužitia alebo neoprávneného použitia platobného prostriedku alebo osobného bezpečnostného prvku

a) Neautorizovanú alebo nesprávne vykonanú platobnú transakciu, stratu, odcudzenie, zneužitie alebo neoprávnené použitie Vášho platobného prostriedku alebo osobného bezpečnostného prvku, osobných dokladov, mobilného telefónu s uloženou platobnou kartou,

s aktivovaným mobilným bankovníctvom alebo čokoľvek podozrivé v súvislosti s internetovým alebo mobilným bankovníctvom nám bezodkladne, najneskôr však do 10 dní, nahláste na Infolinku UniCredit Bank: +421 2 6920 2090 (24/7, nonstop) alebo na ktorejkoľvek našej pobočke v rámci otváracích hodín.

b) Stratu finančných prostriedkov vzniknutú z neautorizovanej platobnej transakcie nesiete do sumy zodpovedajúcej 50 eurám, ak bola táto strata spôsobená použitím strateného alebo odcudzeného platobného prostriedku alebo osobného bezpečnostného prvku alebo zneužitím platobného prostriedku alebo osobného bezpečnostného prvku, ak sú súčasne splnené tieto podmienky:

   (i) Vami neautorizovaná platobná transakcia bola vykonaná potom, ako ste nahlásil(a) UniCredit Bank stratu, odcudzenie, zneužitie alebo neoprávnené použitie platobného prostriedku alebo osobného bezpečnostného prvku, a
   (ii) úmyselne, ani v dôsledku hrubej nedbanlivosti ste neporušil(a) povinnosť chrániť osobné bezpečnostné prvky.

c) Stratu finančných prostriedkov, ktorá vznikla z neautorizovanej platobnej transakcie, nesiete v plnom rozsahu, ak ste spôsobil(a) túto stratu svojím podvodným konaním alebo tým, že ste úmyselne alebo v dôsledku hrubej nedbanlivosti porušil(a) povinnosť chrániť osobné bezpečnostné prvky. Za úmyselné porušenie povinnosti chrániť osobné bezpečnostné prvky alebo za porušenie povinnosti chrániť osobné bezpečnostné prvky v dôsledku hrubej nedbanlivosti sa považuje nedodržanie pravidiel uvedených v tomto dokumente, ako aj vo všeobecne záväzných právnych predpisoch.

10. Zodpovednosť za nesprávne vykonanú platobnú transakciu

O nesprávne vykonanú platobnú transakciu ide vtedy, ak Banka nezúčtovala sumu platobnej transakcie v správnej mene alebo nepoužila číslo účtu alebo iný jedinečný identifikátor v súlade s Vaším príkazom.

Ak má UniCredit Bank povinnosť napraviť nesprávne vykonanú platobnú transakciu a Vy jej oznámite, že netrváte na vykonaní platobnej transakcie, UniCredit Bank bezodkladne:

a) uvedie Váš účet do stavu, v ktorom by bol, ak by toto odpísanie nenastalo, alebo
b) vráti na Váš účet sumu, ako aj poplatok za prevod sumy a ušlé úroky, ak postup podľa písmena a) nepripadá do úvahy.

Ak neoznámite UniCredit Bank, že netrváte na vykonaní platobnej transakcie, UniCredit Bank bezodkladne:
a) zabezpečí pripísanie sumy nesprávne vykonanej platobnej transakcie na účet poskytovateľa platobných služieb príjemcu, a
b) uvedie Váš účet do stavu, v ktorom by bol, ak by UniCredit Bank vykonala platobnú transakciu správne, alebo
c) vráti Vám nesprávne zaplatený poplatok a ušlé úroky, ak postup podľa písmena a) nepripadá do úvahy.