

Opatření proti praní peněz, obcházení mezinárodních sankcí a pro zajištění bezpečnosti klientských operací

Jednou z nejvýznamnějších zákonných povinností UniCredit Bank Czech Republic and Slovakia, a.s. (dále též „Banka“), je aktivně vyhledávat a zamezovat případům legalizace výnosů z trestné činnosti a financování terorismu (dále jen „praní peněz“). Při uplatňování těchto opatření je každý z klientů ze zákona povinen poskytnout Bance součinnost. V rámci aktivit směřujících k zamezení praní peněz má Banka zejména povinnost:

1) provádět **identifikaci** a **kontrolu** klienta

Identifikace klienta je úkon, který musí vždy předcházet jednotlivému obchodu nebo obchodnímu vztahu, jehož obsahem je poskytnutí produktu nebo služby klientovi. Spočívá v získání identifikačních údajů, kterými jsou u:

- a) fyzické osoby nepodnikající - všechna jména a příjmení; rodné číslo, a nebylo-li přiděleno, datum narození; místo narození, pohlaví; trvalý nebo jiný pobyt; státní občanství;
- b) fyzické osoby podnikající - navíc obchodní firmu, odlišující dodatek nebo další označení, místo podnikání a identifikační číslo osoby;
- c) právnické osoby - obchodní firma nebo název vč. odlišujícího dodatku nebo dalšího označení; sídlo; identifikační číslo osoby nebo obdobné číslo přidělené v zahraničí; u fyzických osob, které jsou členem jejího statutárního orgánu údaje fyzické osoby nepodnikající;
- d) svěrenského fondu nebo jiného právního uspořádání bez právní osobnosti - označení a identifikační údaje správce, obhospodařovatele nebo osoby v obdobném postavení.

Až na zákonem vymezené výjimky musí identifikace probíhat za fyzické přítomnosti klienta, přičemž fyzická osoba předkládá při identifikaci průkaz totožnosti a právnická osoba doklad prokazující její existenci. Banka je oprávněna pořizovat kopie dokladů předložených při identifikaci. Kopii průkazu totožnosti pořizuje Banka jen se souhlasem jeho držitele, v případě nesouhlasu provede opis údajů do Identifikační karty.

Kontrola klienta je postup daný Bance zákonem pro účely zjištění údajů nezbytných pro posouzení možného rizika praní peněz. Účelem kontroly je především získání informací o účelu a zamýšlené povaze obchodu nebo obchodního vztahu, informací o zdroji peněžních prostředků, kterých se obchod nebo obchodní vztah týká a informací potřebných pro průběžné sledování obchodního vztahu. Kontrola zahrnuje rovněž zjišťování tzv. skutečného majitele, tedy fyzické osoby, která vykonává fakticky nebo právně rozhodující vliv v právnické osobě nebo svěrenském fondu.

2) naplňovat své povinnosti v rámci uplatňování **mezinárodních sankcí**

Mezinárodní sankce představují souhrn omezujících opatření, jež mezinárodní společenství (OSN, EU) používají jako nástroj k udržení nebo obnovení mezinárodní míru a bezpečnosti, k ochraně základních lidských práv a k boji proti terorismu. Banka má v této souvislosti povinnost řídit se omezeními či zákazy poskytování jakýchkoli plnění subjektům, na které se vztahují mezinárodní sankce, uzavírání obchodů s nimi, včetně obchodů s cizí měnou, převodů peněžních prostředků aj. Banka má v těchto případech právo odmítnout vstup do smluvního vztahu či smluvní vztah jednostranně ukončit.

3) uplatňovat zvláštní postupy vůči **politicky exponovaným osobám**

Politicky exponovanou osobou je fyzická osoba, která je nebo byla ve významné veřejné funkci s celostátním nebo regionálním významem. Banka má ze zákona

povinnost provést u této osoby vždy kontrolu zahrnující nejen získání informací o účelu obchodu či obchodního vztahu, o zdroji peněžních prostředků, kterých se obchod či obchodní vztah týká, ale v rámci přiměřených opatření též informací o původu jejího majetku, v průběhu obchodního vztahu.

Banka se dále aktivně snaží bránit útokům na produkty klientů, které jsou uskutečňovány za účelem získání jejich peněžních prostředků a které jsou v současné době prováděny ve významné míře v prostředí internetu. Rovněž při bránění těmito aktivitám je nutná spolupráce klientů a dalších osob, které jsou s Bankou v jiném vztahu nebo osob, které pokusy o výše uvedené aktivity zjistí. V této souvislosti jsou nejčastěji se vyskytujícími útoky následující:

- a) **phishing** - útok prováděný e-mailem tak, že se útočník snaží přesvědčit klienta, aby otevřel přílohu či kliknul na link odkazující na pro tento účel vytvořenou internetovou stránku, prezentující se například jako výzva k aktualizaci bezpečnostních údajů, informace o neprovedení platby či dokonce jako výzkum klientské spokojenosti, s cílem získat klientova hesla do internetového bankovníctví nebo PIN k platební kartě;
- b) **CEO fraud** - útoky prováděné e-mailem tak, že se útočník vydává za osobu v řídicí funkci společnosti či jejího obchodního partnera a kontaktuje pracovníka firmy s přístupem k jejím financím s požadavkem na jejich převod na útočnickem připravený účet;
- c) **social engineering** - útok využívající manipulaci oběti k jednání, kterého by se za normálních okolností nedopustila (např. klientův zavírovaný počítač prezentuje falešná upozornění s požadavkem na změnu hesla do internetového bankovníctví; telefonující se vydává za osobního bankéře ve snaze získat přístupové údaje do internetového bankovníctví klienta) a další.

V této souvislosti je zásadní, aby klient zejména:

- nikomu nesděloval hesla do svého internetového bankovníctví či ke svým platebním prostředkům;
- přistupoval do svého internetového bankovníctví pouze z bezpečných zařízení a nikoli přes veřejné internetové sítě;
- do internetového bankovníctví přistupoval pouze přes zabezpečené připojení (adresa s „https://“, nikoli jen „http://“, na počátku příkazového řádku prohlížeče);
- aktualizoval software svého zařízení umožňujícího přístup do internetového bankovníctví a používal vhodné antivirové programy;
- měl přehled a průběžně sledoval zůstatek na svém účtu;
- přistupoval pouze na známé internetové stránky.

V případě, že zpozorujete cokoliv podezřelého v souvislosti s Vaším internetovým nebo mobilním bankovníctvím, žádáme Vás, abyste okamžitě kontaktovali klientskou linku Banky 800 14 00 14.

Vážení klienti,

doufáme ve vzájemné pochopení, vstřícnost a důvěru při realizaci Vašich požadavků, ale i požadavků zákona o praní peněz a obecných principů bezpečnosti, které stanoví rámec vzájemného úspěšného jednání.

S úctou,

UniCredit Bank Czech Republic and Slovakia, a.s.

13.10.2017