Smlouva o zajištění bezpečnosti provozu platebních terminálů

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku

Československá obchodní banka, a. s.

se sídlem Radlická 333/150, 150 57 Praha 5

IČO 000 01 350

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl BXXXVI, vložka 46, zastoupená …….

(dále jen „**Banka**“ nebo „**ČSOB**“)

a

Název společnosti,

se sídlem .....,

IČO ....., DIČ: .....

zapsaná v obchodním rejstříku vedeném ....., zastoupená …..

(dále jen „**Dopravce**”)

Čl. I. Předmět smlouvy

1. ČSOB jako zúčtovací banka karetních asociací je zodpovědná vůči karetním asociacím za dodržování bezpečnostních standardů stanovených těmito asociacemi a dalšími pravidly, která jsou karetními asociacemi vyžadovány, jako např. tzv. Payment Card Industry Data Security Standard (dále jen PCI DSS).
2. Předmětem této smlouvy je stanovení bezpečnostních podmínek provozu validátorů/odbavovacích zařízení s integrovaným platebním terminálem, příp. externím platebním terminálem, vybaveným bankovní platební aplikací (dále jen „Terminál“). Transakce provedené bankovními platebními kartami na Terminálech jsou zpracovány společností Koordinátor ODIS, s.r.o., IČ: 64613895 se sídlem 28. října 3388/111, 702 00 Ostrava – Moravská Ostrava (dále jen „Koordinátor“). Koordinátor vybral pro zúčtování transakcí provedených bankovními platebními kartami partnera, jehož zúčtovací bankou bankovních platebních karet je ČSOB.
3. Dopravce bere na vědomí, že bezpečnostní požadavky karetních asociací prochází pravidelnou aktualizací v souvislosti s aktuálními hrozbami a mohou se objevit nové požadavky, které musí Dopravce implementovat. V takovém případě se ČSOB zavazuje Dopravce seznámit s těmito aktualizovanými pravidly a Dopravce se zavazuje bezodkladně upravit postupy pro provádění bezpečnostních kontrol.

Čl. II. Závazky Dopravce a ČSOB na zajištění bezpečnosti provozu

A. Požadavky na plnění PCI DSS

1. Dopravce se zavazuje seznámit se s pravidly PCI DSS v aktuální verzi, která jsou aplikovatelná pro prostředí Dopravce (v originálním znění dostupné na www.pcisecuritystandards.org, v českém jazyce pak na www.pcistandard.cz). Přehled aktuálně platných pravidel je uvedený v Příloze 1 této Smlouvy. Při každé případné změně verze standardu PCI DSS sdělí tyto skutečnosti ČSOB Dopravci. Dopravce se zavazuje v souvislosti s výše uvedeným:
   a) splňovat a bezvýjimečně dodržovat všechny požadavky PCI DSS dle úrovně, do které byl na základě kritérií zařazen. Úroveň je Dopravci oznámena písemně ze strany ČSOB spolu s rozsahem požadavků aplikovatelnými na Dopravce,
   b) žádným způsobem nezpracovávat, nepřenášet nebo neuchovávat jakákoli data uvedená na platebních kartách. Výjimku tvoří prvních 6 a poslední 4 číslice z čísla karty, které je možné zpracovávat pro interní účely, např. reklamace,
   c) zajistit ochranu dat držitelů platebních karet, která jsou zpracována, uložena nebo přenesena přes systémy provozované Dopravcem a nést v plné výši odpovědnost za veškeré škody vzniklé jejich případnou ztrátou či zneužitím,
   d) umožnit ČSOB, případně asociacím, kontrolovat plnění souladu s PCI DSS,
   e) zajistit vyplnění PCI-DSS Self-Assessment Questionare dotazníku (dále jen „SAQ dotazník“) podle úrovně, do které je ze strany ČSOB zařazen v souladu s PCI-DSS předpisy. Dotazník poskytne ČSOB v českém jazyce a Dopravce jej bude vyplňovat rovněž v českém jazyce.
2. Dopravce se zavazuje zajistit proškolení všech osob, jež přichází do styku s Terminálem (např. řidiči a servisní pracovníci) v návaznosti na provádění kontrol popsaných níže v článku II, písm. B).
3. Dopravce si je vědom, že v případě jím nezajištěného souladu s pravidly PCI DSS, pokud dojde ke vzniku škody, pak Dopravce za tuto škodu nese odpovědnost.
   V případě jakéhokoliv bezpečnostního incidentu na Terminálech (ztráta, zcizení, neautorizovaná modifikace, neoprávněná manipulace, apod.) se zavazuje Dopravce bezodkladně informovat ČSOB na adresu akceptacekaret@csob.cz. Takovou informaci je ČSOB oprávněna dále sdílet s karetními asociacemi, příslušnými státními orgány a s dalšími dotčenými stranami.
4. Dopravce bere na vědomí, že ČSOB v rámci bezpečnostního a provozního monitoringu může přistoupit vzdáleně k platební aplikaci v Terminálu a provést nezbytné servisní zásahy, které zajistí fungování platební aplikace v terminálu. Dopravce bere na vědomí, že v případě podezření na bezpečnostní incident je ČSOB oprávněna POS aplikaci vzdáleně deaktivovat a znemožnit akceptaci bankovních karet. ČSOB bude o zásahu bezodkladně informovat Dopravce, nejpozději do 10 minut od provedení zásahu.
5. Dopravce bere na vědomí, že ČSOB v případě identifikace podezřelých nebo protiprávních aktivit bezodkladně informuje Dopravce o této skutečnosti a Dopravce se zavazuje bezodkladně učinit opatření, která povedou k účinnému nebo alespoň adekvátnímu omezení takových aktivit. Dopravce bere na vědomí, že v případech, kdy dochází k rozsáhlému nebo intenzívnímu nebo zřejmě organizovanému páchání protiprávní činnosti nebo v případech, kdy hrozí poškození dobrého jména ČSOB nebo Dopravce, je ČSOB oprávněna na nezbytně nutnou dobu podle povahy věci omezit nebo pozastavit fungování akceptace bankovních platebních karet na Terminálech. Dopravce přičemž odbavení na Moravskoslezskou kartu ODISka zůstává funkční. ČSOB bude o zásahu bezodkladně informovat Dopravce, nejpozději do 10 minut od provedení zásahu.

B. Požadavky na fyzickou kontrolu Terminálů (validátorů / odbavovacích zařízení)

Dopravce se zavazuje provádět periodické bezpečnostní kontroly, minimálně však 1x týdně, které mají za cíl ověřit přítomnost neautorizovaného zařízení. Kontroly je povinen Dopravce provádět minimálně v následujícím rozsahu:

a) že Terminál není viditelně poškozen a nenese známky narušení ochranného krytu. Celá sestava působí celistvým dojmem a není možné oddělit některou jeho část,
b) že Terminál neobsahuje viditelně nějaké další zařízení jako např. nejrůznější modifikované nástavce, případně doplňky připevněné k validátoru/odbavovacímu zařízení, které mohou potenciálně obsahovat čtecí zařízení pro vyčítání karetních dat, případně klávesnici pro zadávání PINů ke kartám,
c) že veškerá manipulace s Terminálem (např. instalace do vozů, odinstalace) je prováděna pouze pověřenými osobami Dopravce.

Kontrolu je povinen Dopravce provádět minimálně po dobu, kdy bude provozovat Terminál vybavený aktivní bankovní platební aplikací ČSOB.

Čl. III. Ujednání o náhradě škod

1. Každá ze smluvních stran nese odpovědnost za, z její strany, způsobenou škodu při porušení platných právních předpisů a této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

Čl. IV. Ukončení smlouvy

1. Smlouva může být ukončena dohodou smluvních stran.
2. Smlouva může být ukončena výpovědí, a to bez uvedení důvodu. Výpovědní doba je na straně ČSOB 3 měsíce, na straně Dopravce 3 měsíce a počíná běžet ode dne doručení výpovědi druhé smluvní straně.
3. Od Smlouvy může ČSOB odstoupit s okamžitou platností, počínaje dnem doručení písemného vyrozumění Dopravci, a to v případě podstatného porušení Smlouvy Dopravcem, kterým se rozumí opakované porušení jakékoli jeho povinnosti vyplývající z této Smlouvy.
4. Od Smlouvy může Dopravce odstoupit s okamžitou platností, počínaje dnem doručení písemného vyrozumění ČSOB, a to v případě podstatného porušení Smlouvy ČSOB, kterým se rozumí opakované porušení jakékoli jeho povinnosti vyplývající z této Smlouvy.
5. V případě, že se výpověď či vyrozumění o odstoupení od Smlouvy nepodaří doručit z důvodů na straně druhé smluvní strany (např. nepřebírá zásilku), a písemnost bude Českou poštou, s. p., vrácena jako nedoručitelná, účinky doručení nastávají v den, kdy bude zásilka vrácena smluvní straně, která zásilku odeslala.

Čl. V. Závěrečná ustanovení

1. Smlouva se sjednává na dobu neurčitou s možností jejího ukončení dle článku IV.
2. Smlouva je vypracována ve 4 vyhotoveních v českém jazyce s tím, že každá ze smluvních stran obdrží po dvou vyhotoveních.
3. Jakékoli změny a doplňky této Smlouvy lze provést pouze na základě souhlasu obou smluvních stran formou písemného číslovaného dodatku, který bude součástí této Smlouvy.

4. ČSOB a Dopravce dále sjednávají, že bude-li jakékoliv ustanovení této Smlouvy nebo jeho část shledáno soudem či jiným kompetentním orgánem z jakéhokoli důvodu neplatným nebo nevymahatelným, bude se aplikovat s nezbytnou minimální úpravou tak, aby bylo platné a účinné a platnost nebo vymahatelnost zbývajících ustanovení této Smlouvy nebude nijak dotčena ani oslabena.
5. Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oprávněnými zástupci obou smluvních stran.
6. Nedílnou součástí této Smlouvy jsou i její přílohy:

   Příloha 1 - Aplikovatelné požadavky PCI DSS v. 3.1

Za ČSOB:	Za Dopravce:
V Praze dne	V …….. dne

Příloha 1 Aplikovatelné požadavky PCI DSS v. 3.1

PCI DSS Otázka	Testovací procedura	Vysvětlení
9.9 Chránit zařízení, která snímají data platebních karet prostřednictvím přímé fyzické interakce s kartou, před manipulací a substitucí (nahrazením). ***Poznámka**: Tyto požadavky se vztahují na čtecí zařízení karet používaných při transakcích za přítomnosti karet (to znamená, že karta je protažena nebo vložena) v místě prodeje. Tento požadavek není určen k aplikaci pro zařízení, které využívá manuální vkládání dat, jako jsou počítačové klávesnice a POS klávesnice.* ***Poznámka**: Požadavek 9.9 je pokládán za osvědčený postup do 30. června 2015, po tomto datu se stává požadavkem.*	**9.9** Zkontrolovat dokumentované politiky a procedury a ověřit, zda zahrnují: □ Udržování seznamu zařízení. □ Provádět pravidelně prohlídku zařízení a prozkoumat, zda s ním nebylo manipulováno nebo nebylo nahrazeno. □ Školení pracovníků, aby si byli vědomi podezřelého chování a nahlásili nedovolenou manipulaci nebo náhradu zařízení.	Zločinci se pokoušejí ukrást data držitelů karet krádeží a/nebo manipulací se čtecím zařízením karet a terminálů. Například se budou snažit ukrást zařízení, aby se mohli naučit, jak do něj proniknout, a často se snaží na hradit legitimní zařízení zařízením podvodným, které jim posílá informace o platební kartě pokaždé, když je karta vložena. Zločinci se také snaží připojit komponenty pro "skimming" zvnějšku zařízení, které jsou určeny k zachycení údajů z platební karty ještě před tím, než je karta vložena do zařízení. Například připojením dodatečné čtečky karet nad legitimní čtečku karet tak, aby údaje platebních karet byly zachyceny dvakrát: jednou komponentou zločince a pak legitimní komponentou zařízení. Tímto způsobem transakce může být dokončena bez přerušení, zatímco zločinec si během procesu "naskimuje" (načte) údaje o platební kartě. Tento požadavek se doporučuje, ale není vyžadován pro zařízení, které využívá manuální vkládání dat, jako jsou počítačové klávesnice a POS klávesnice. Další osvědčené postupy v prevenci skimmingu jsou k dispozici na internetových stránkách PCISSC.
9.9.1 Udržovat aktuální seznam zařízení. Seznam by měl zahrnovat následující body: □ Značku a model zařízení □ Umístění zařízení (např. adresa místa nebo objektu, kde se zařízení nachází) □ Sériové číslo zařízení nebo jiný způsobu nikátní identifikace.	**9.9.1.a** Zkontrolovat seznam zařízení a ověřit, zda obsahuje: □ Značku a model zařízení □ Umístění zařízení (např. adresa místa nebo objektu, kde se zařízení nachází) □ Sériové číslo zařízení nebo jiný způsob unikátní identifikace. **9.9.1.b** Vybrat vzorek zařízení ze seznamu a sledovat zařízení a umístění zařízení a ověřit, zda je seznam přesný a aktuální. **9.9.1.c** Dotázat se pracovníků a ověřit, zda je seznam zařízení aktuální, když jsou zařízení přidána, přemístěna, vyřazena z provozu, atd.	Vedení aktuálního seznamu zařízení napomáhá organizaci sledovat, kde by se zařízení mělo nacházet a rychle určit, zda zařízení chybí nebo je ztraceno. Způsob udržování seznamu zařízení může být automatizováno (například systémem pro správu zařízení) nebo manuálně (například dokumentace pomocí elektronických nebo papírových záznamů). Pro putovní zařízení (“na cestě”)můžeme namísto umístění uvést jména pracovníků, jimž byla zařízení přidělena.

9.9.2 Pravidelně kontrolovat povrchy zařízení a detekovat neoprávněnou manipulaci (např. přidání skimmeru-nelegální čtečky Karet do zařízení) nebo výměnu(např. kontrolou sériového čísla nebo jiné vlastnosti zařízení ověřit, zda zařízení nebylo vyměněno za podvodné zařízení). ***Poznámka**: Příklady příznaků, které naznačují, že se zařízením mohlo být manipulováno nebo bylo nahrazeno, jsou neočekávané přílepky nebo kabely zapojené do zařízení, chybějící nebo změněné bezpečnostní štítky, zlomené nebo jinak barevné kryty nebo změny v sériovém čísle zařízení nebo jiné vnější znaky.*	**9.9.2.a** Zkontrolovat dokumentované procedury a ověřit, zda procesy jsou definovány tak, aby obsahovaly následující body: □ Procedury pro provedení prohlídky zařízení □ Frekvenci kontrol.	Pravidelné prohlídky zařízení napomohou organizacím rychleji detekovat neoprávněnou manipulaci nebo výměn u zařízení, a tím minimalizovat potenciální Dopad používání podvodných zařízení. Typ prohlídky bude záviset na zařízení, například fotografie zařízení, o kterém je známo, že je bezpečné, mohou být použity pro srovnání aktuálního vzhledu přístroje s jeho původním vzhledem, aby se zjistilo, zda se vzhled změnil. Další možností může být použití bezpečného popisovače, jako je značkovač viditelný pod UV zářením, k označení povrchů zařízení a otvorů v zařízení, takže jakákoliv neoprávněná manipulace nebo výměna bude zřejmá. Zločinci často nahradí vnější kryt zařízení, aby skryli manipulaci, a tyto metody mohou napomoci odhalit takovéto činnosti. Dodavatelé zařízení mohou být také schopni poskytnout bezpečnostní pokyny a návody, jak napomoci rozhodnutí, zda bylo se zařízením manipulováno. Četnost prohlídek bude záviset na faktorech, jako je umístění zařízení a zda je zařízení obsluhováno nebo bez dozoru. Například zařízení, ponechaná ve veřejných prostorách bez dohledu pracovníků organizace, mohou mít častější prohlídky než zařízení, která jsou umístěna v zabezpečených oblastech nebo jsou-li přístupné veřejnosti pod dohledem. Typ a četnost prohlídek bude určena obchodníkem, jak jsou definovány v ročním procesu analýze rizik.
	9.9.2.b Dotázat se odpovědných pracovníků, sledovat postupy prohlídek a ověřit: □ Pracovníci si jsou vědomi postupů pro prohlídky zařízení. □ Všechna zařízení jsou pravidelně prohlížena a jsou hledány důkazy o manipulaci a substituci (nahrazení).	
9.9.3 Zajistit školení pro pracovníky, aby si byli vědomi pokusů o manipulaci se zařízením nebo jejich výměně. Školení by mělo zahrnovat následující body: □ Ověřit identitu jakýchkoli osob třetí strany, kteří tvrdí, že jsou pracovníci opravy nebo údržby, před udělením přístupu k provedení opravy nebo údržby zařízení. □ Neinstalovat, nevyměňovat ani nevracet zařízení bez ověření. □ Být si vědom podezřelého chování kolem zařízení (např. pokusy neznámých osob o odpojení nebo otevření zařízení). □ Hlásit podezřelé	**9.9.3.a** Prověřit školící materiály pro pracovníky v místě prodeje a ověřit, zda jsou školení v následujících bodech: □ Ověřit identitu jakýchkoli osob třetí strany, kteří tvrdí, že jsou pracovníci opravy nebo údržby, před udělením přístupu k provedení opravy nebo údržby zařízení. □ Neinstalovat, nevyměňovat ani nevracet zařízení bez ověření. □ Být si vědom podezřelého chování kolem zařízení (např. pokusy neznámých osob o odpojení nebo otevření zařízení). □ Hlásit podezřelé chování a známky manipulace se zařízením nebo jeho výměnu příslušným pracovníkům (například manažerovi nebo bezpečnostnímu pracovníkovi).	Zločinci se často představují jako pracovníci pověření údržbou za účelem získání přístupu k POS zařízením. Všechny třetí strany, požadující přístup k zařízením, by měly být vždy ověřeny před umožněním přístupu - například kontrolou u vedení nebo telefonicky ověřit se společností zajišťující údržbu POS zařízení (například dodavatel nebo acquirer). Mnozí zločinci se budou snažit oklamat pracovníky oblečením pro svou roli (např. nošením boxu s nářadím a pracovním oblečením), a mohou být také dobře informováni o umístění zařízení, takže je důležité, aby pracovníci byli vyškoleni a vždy se chovali v souladu s procedurami. Dalším trikem, kteří zločinci rádi používají, je zaslání "nového" systému POS s pokynem jej zaměnit za legitimní systém a "vrácení" legitimního systému na zadanou adresu. Zločinci mohou dokonce poskytnout zpáteční poštovné, protože by velice rádi dostali do svých rukou tato zařízení. Pracovníci vždy musí ověřit u svého manažera nebo dodavatele, že zařízení je legitimní a pochází z důvěryhodného zdroje, a to ještě před instalací nebo jeho použitím v provozu.

chování a známky manipulace se zařízením nebo jeho výměnu (substituci) příslušným pracovníkům (například manažerovi nebo bezpečnostnímu pracovníkovi)	**9.9.3.b** Dotázat se vzorku pracovníků v místě prodeje a ověřit, zda absolvovali školení a jsou si vědomi procedur pro následující body: Ověření identity jakýchkoli osob třetích stran, kteří tvrdí, že jsou pracovníci opravy nebo údržby, před udělením přístupu k provedení změn nebo údržby zařízení. Neinstalovat, nevyměňovat ani nevracet zařízení bez ověření. Být si vědom podezřelého chování kolem zařízení (např. pokusy neznámých osob o odpojení nebo otevření zařízení). Hlásit podezřelé chování a známky manipulace se zařízením nebo jeho výměnu příslušným pracovníkům (například manažerovi nebo bezpečnostnímu pracovníkovi).	