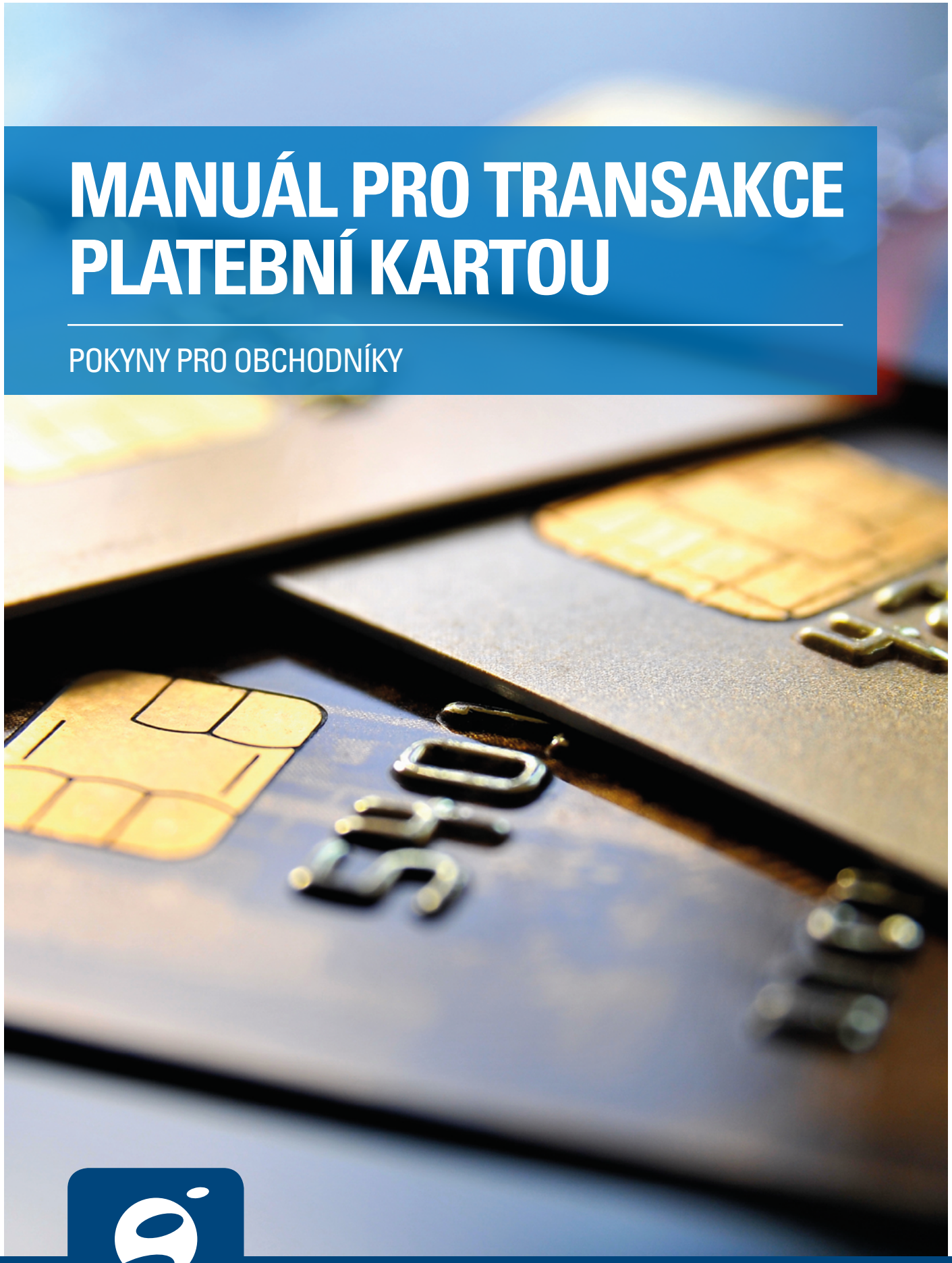
MANUÁL PRO TRANSAKCE PLATEBNÍ KARTOU

POKYNY PRO OBCHODNÍKY



SERVICE. DRIVEN. COMMERCE

globalpaymentsinc.com

Ve spolupráci s

OBSAH

VÍTEJTE

Jsme rádi, že jste se stali zákazníkem společnosti Global Payments, jejímž jediným a jednoduchým cílem je poskytnout Vám bezpečné a spolehlivé služby v oblasti zpracování karetních transakcí, kdy za Vaše peníze dostanete skutečnou hodnotu.

Znamená to úzkou spolupráci s Vámi.

Pozorně naslouchámе, co nám říkáte o svých potřebách, a to nám pomáhá důkladně porozumět Vašemu podnikání. Budeme se snažit spolupracovat s Vámi profesionálním, transparentním a férovým způsobem. Váš názor na naše služby je pro nás důležitý, budeme rádi, když se s námi o něj podělíte.

O NÁS

1. června 2016 uzavřely společnosti Global Payments Inc., přední světový poskytovatel služeb v oblasti technologií pro zpracování plateb, CaixaBank, největší španělská banka dle tržního podílu, a Erste Group, přední poskytovatel finančních služeb ve střední a východní Evropě, dohodu o vzájemné spolupráci při získávání zákazníků z řad obchodníků a v oblasti platebních služeb v České republice, na Slovensku a v Rumunsku.

Výsledkem Smlouvy bylo založení samostatné právnické osoby s názvem Global Paymetns s.r.o., která funguje nezávisle na společnosti Global Payments Europe, s.r.o. (GPE), která je nicméně jejím partnerem v technické oblasti, v oblasti inovací a v poskytování služeb podpory pro obchodníky.

Společnost Global Payments vyvíjí svá řešení na základě potřeb zákazníků po celém světě a je vyhledávaným partnerem díky tomu, že poskytuje široké portfolio produktů a služeb, které pomáhají jejím zákazníkům v růstu a inovaci. Ať už je to osobně, online nebo „za pochodu“, vždy Vám nabízíme svou odbornou pomoc při hledání a implementaci unikátních řešení v oblasti platebních služeb.

Jakožto společnost, která se soustředí na služby a obchod, vynakládá Global Payments maximální úsilí, aby byla odpovědným členem komunity, a naši zaměstnanci prokazují vášeň a nadšení pro pozitivní změny v životech druhých. Jsme součástí globálního podnikatelského společenství a náš vztah k okolní komunitě je klíčový pro hodnoty, které naše společnost zastává, a pro to, kdo jsme: po celém světě se snažíme přispívat k pozitivním změnám tím, že nabízíme svůj čas, služby a finanční pomoc lidem, kteří to potřebují.

O SPOLEČNOSTI GLOBAL PAYMENTS

Global Payments Inc. je předním světovým poskytovatelem v oblasti platebních služeb, dodávající inovativní řešení šitá na míru zákazníkům na celém světě. Naše technologie, partneři a odbornost našich zaměstnanců nám umožňují dodávat rozsáhlý výběr produktů a služeb tak, aby naši zákazníci mohli využívat všechny nástroje z oblasti akceptace a zpracování plateb prostřednictvím platebních karet napříč různými distribučními kanály v mnoha tržních prostředích celého světa.

Global Payments sídlící v Atlantě (stát Georgia, USA) zaměstnává více než 8500 lidí po celém světě, je zařazená do seznamu S&P 500 a má své partnery a zákazníky ve 30 zemích v celé Severní Americe, Evropě, Asia-Pacific regionu a v Brazílii. Pro více informací o společnosti Global Payments, značky Service.Driven. Commerce a jejích technologiích, prosím navštivte stránku www.globalpaymentsinc.com.

O TOMTO DOKUMENTU

Tyto Pokyny pro obchodníky spolu s dalšími dokumenty uvedenými v bodu 1. 1. *Všeobecných obchodních podmínek* představují Smlouvu o akceptaci platebních karet, kterou s námi uzavíráte (dále jako „Smlouva“).

Ve svém vlastním zájmu a pro svou vlastní ochranu byste měli tento dokument pozorně přečíst, neboť tvoří součást Smlouvy, o kterou se hodláme opírat. Pokud jakémukoliv bodu nerozumíte, vyžádejte si prosím další informace. Naše kontaktní údaje jsou uvedeny na straně 54.

Co se dozvíte v tomto manuálu pro obchodníky?

Tento manuál Vám poskytne:

- přehled různých způsobů, jak můžeme podpořit Vaše podnikání
- provozní pokyny
- důležité informace o rizicích spojených s užíváním

a akceptací karet; manuál uvádí užitečné tipy a rady, které je důležité dodržovat během akceptace platebních karet

- manuál Vám umožní efektivně provádět karetní transakce a těžit tak ze svého nového zařízení na zpracování transakcí platební kartou.

Přečtěte si prosím tento dokument pozorně: obsahuje klíčové informace, které Vám mohou pomoci v prevenci fraudů a chargebacků

Dodržujte prosím důkladně postupy podrobně popsané v tomto manuálu. Díky nim budete moci Vy a Vaše podnikání maximálně těžit z přijímání platebních karet.

Měli byste rovněž mít na vhodném místě k dispozici kopii těchto Pokynů pro obchodníky, aby byla v případě potřeby snadno dostupná Vám a Vašim zaměstnancům. Pokud nemůžete nalézt informace, které potřebujete, kontaktujte nás prosím (viz strana 54, kde jsou uvedeny kontaktní údaje).

Informujte nás prosím o změnách ve Vašem podnikání

S přijímáním platebních karet jsou spojena rizika a my cítíme, že naší povinností je zajistit, že jste si těchto rizik vědomi. Budeme Vás informovat o vývoji v tomto odvětví včetně trendů v podvodné činnosti a pokrocích v procesech a technologiích zaměřených na boj proti podvodům. Pomůžeme Vám tím udržet bezpečnost na nejvyšší možné úrovni a snížit riziko hrozící Vašemu podnikání.

Abychom Vám mohli poskytovat aktuální informace a zajistili, že dostáváte odpovídající služby, dejte nám prosím vědět, pokud se některý z níže uvedených údajů o Vašem podnikání změní, např.:

- Vaše kontaktní údaje (včetně emailové adresy a telefonního čísla);
- Vaše adresa (včetně Vaší obchodní adresy, korespondenční adresy, adresy Vašeho ústředí atd.);
- Druh podnikání, kterému se věnujete;
- Významné změny v množství obchodních transakcí, které provádíte;
- Zamýšlíte změnit způsob, jakým podnikáte, např. pokud uvažujete o tom, že začnete obchodovat na internetu nebo o tom, že začnete využívat služeb nového Poskytovatele platebních služeb (PSP, Payment Services Provider);
- Významné změny ve vlastnických podílech ve Vaší společnosti (za významnou se obvykle považuje změna týkající se více jak 25% podílu); nebo
- Pokud prodáte svůj podnik nebo měníte jeho právní formu.

K tomu, abyste nás informovali o jakékoliv z výše uvedených změn, prosím využijte naši nonstop zákaznickou linku (viz str. 54) nebo změnový formulář, který je k dispozici ke stažení v Merchant Portálu.

Neváhejte nás prosím kontaktovat s jakýmikoliv otázkami nebo zpětnou vazbou.

Našim cílem je poskytnout Vám nejkvalitnější možné služby. Proto vítáme veškeré Vaše připomínky a zpětnou vazbu. Neváhejte nás prosím kontaktovat, máte-li jakékoliv otázky či připomínky týkající se těchto pokynů či jakéhokoliv aspektu námi poskytovaných služeb. Naše kontaktní údaje naleznete na str. 54.

DEFINICE NĚKTERÝCH POJMŮ

AS
Autorizační servis – místo, kde jsou realizovány autorizační požadavky plateb.

ASOCIACE
Mezinárodní společnost udílející bankám licence na vydávání a zpracovávání transakcí uskutečněných platebními kartami (Visa Intl., Mastercard Intl., Diners Club Intl., Japan Credit Bureau Intl., American Express Intl.).

AUTORIZACE
Proces ověření možnosti uskutečnit bezhotovostní platbu prostřednictvím platební karty. Slouží k ověření platnosti karty a krytí kartové transakce.

AUTORIZAČNÍ KÓD
Čtyř- až šestimístná kombinace číslic (u společnosti American Express pouze dvoumístná) nebo číslic a písmen, která je obchodnímu partnerovi sdělena jako reference vydaného souhlasného oprávnění s provedením kartové transakce.

AUTORIZAČNÍ LIMIT
Maximální výše částky (defaultně 0,00 Kč), na kterou lze uskutečnit prostřednictvím jedné platební karty na jednom obchodním místě Obchodníka během jednoho kalendářního dne, aniž by bylo bezpodmínečně nutné vyžadovat oprávnění ke kartové transakci prostřednictvím AS. Výše částky může být změněna pro některé segmenty, na základě žádosti zaslané PPS.

BEZKONTAKTNÍ TECHNOLOGIE (CONTACTLESS) Bezkontaktní akceptace platebních karet. U bezkontaktních plateb je na platební kartě vyobrazen kromě standardních bezpečnostních prvků také symbol, který opravňuje držitele karty provádět bezkontaktní transakce.

BEZKONTAKNÍ ČTEČKA
Bezkontaktní čtecí zařízení umístěné mimo platební terminál nebo součástí platebního terminálu vyvinuté pro přijímání platebních karet a jiných zařízení s bezkontaktní technologií.

ČIP
Mikroprocesor umístěný na přední straně platební karty. Jeví se jako kovová ploška oválného nebo obdélníkového tvaru.

DYNAMIC CURRENCY CONVERSION (DCC)
Dynamic Currency Conversion, aplikace na platební terminál (POS), která umožňuje držiteli karty volbu zaplatit za zboží či služby ve své domácí měně.

DRŽITEL KARTY
Fyzická osoba, které byla na základě smlouvy s vydavatelem platebních karet vydána platební karta a jejíž příjmení a jméno jsou vyznačeny na platební kartě.

HYBRIDNÍ PLATEBNÍ KARTA
Platební karta, která v sobě zahrnuje více platebních aplikací jedné kartové asociace (např. debetní a kreditní Visa) nebo může obsahovat více platebních značek kartových asociací.

IMPRINTER
Mechanické zařízení určené k provedení otisku identifikačních údajů embosované platební karty a identifikačního štítku obchodního místa při provádění kartové transakce, které není naší společností podporováno.

MASTERCARD MOBILE
Elektronická platební peněženka v mobilním telefonu zákazníka.

MPOS
Mobilní zařízení pro elektronické přijímání a zpracování kontaktních (magnetický proužek nebo čip) i bezkontaktních kartových transakcí.

NFC TECHNOLOGIE
NFC (Near Field Communication) je bezdrátová technologie – rádiový přenos dat na krátkou vzdálenost, která umožňuje jednoduchou a bezpečnou obousměrnou komunikaci mezi elektronickými zařízeními, jako provádění bezkontaktní transakce např. mobilním telefonem, přívěskem, hodinkami, stickerem, platba přes QR kód apod.

OBCHODNÍ MÍSTO/PRODEJNÍ MÍSTO
Místo, na kterém jsou Obchodníkem přijímány bezhotovostní úhrady prostřednictvím platebních karet, NFC za poskytnuté zboží a služby, adresa na níž se nacházejí prostory Obchodníka a kde byla daná platební transakce iniciována. Avšak a) v případě smluv uzavřených na dálku ve smyslu čl. 2 bodu 7 směrnice 2011/83/EU je prodejním místem adresa trvalého místa

podnikání, na které Obchodník vykonává svou činnost, bez ohledu na umístění internetových stránek nebo serveru, a jejímž prostřednictvím je platební transakce iniciována; b) nemá-li Obchodník trvalé místo podnikán, je prodejním místem adresa, ve vztahu k níž má Obchodník platnou licenci k podnikání a jejímž prostřednictvím je platební transakce iniciována; c) nemá-li Obchodník trvalé místo podnikání ani platnou licenci k podnikání, považuje se za prodejní místo korespondenční adresa, která je stanovena pro účely platby daní související s jeho obchodní činnosti a jejímž prostřednictvím je platební transakce iniciována.

OBSLUHA OBCHODNÍHO MÍSTA
Fyzická osoba, která je pověřena Obchodníkem k přijímání platebních karet a k obsluze příslušných zařízení akceptace platebních karet.

PIN PAD
Externí zařízení pro zadávání PINu, které pracuje samostatní nebo je připojeno k platebnímu terminálu.

PLATBA KARTOU
Kartová transakce prováděná ve prospěch Obchodníka k úhradě kupovaného zboží nebo poskytnutých služeb prostřednictvím platební karty nebo NFC zařízení.

PLATEBNÍ KARTA
Plastová karta, která svým vzhledem, uspořádáním údajů a ochrannými prvky odpovídá z lícové i rubové strany specifikaci stanovené asociací. Prostřednictvím platební karty lze uskutečňovat bezhotovostní platby za zboží a služby a výběr hotovosti.

PLATEBNÍ TERMINÁL (POS)
Elektronický platební terminál pro elektronické přijímání a zpracování kontaktních (magnetický proužek a čip) i bezkontaktních kartových transakcí. Jeho součástí může být i přídavné zařízení pro zadávání PIN, tzv. PIN pad.

PLATNOST KARTY
Doba, v průběhu které může držitel platební kartu využívat k realizaci kartových transakcí. Platnost karty je vyznačena na přední straně platební karty.

PODKLADY K TRANSAKCI
Obecný název pro veškeré dokumenty vztahující se k transakci.

POSKYTOVATEL PLATEBNÍCH SLUŽEB/PPS
Acquirer/Akceptant – dodavatel platebních služeb, který s Obchodníkem uzavírá smlouvu o přijímání platebních karet a dodává služby související s přijímáním platebních karet.

PRODEJNÍ DOKLAD
Papírový nebo elektronický doklad o provedení kartové transakce.

PRŮKAZ TOTOŽNOSTI
Občanský průkaz nebo cestovní pas.

REFUNDACE
Transakce provedená ve prospěch držitele karty, kterou se Obchodník zavazuje vrátit platbu prostřednictvím PPS Držiteli karty za reklamované nebo vrácené zboží.

ÚVOD DO ZPRACOVÁNÍ PLATEB KARTOU

Přijímání platebních karet může Vašemu podnikání přinést řadu výhod včetně:

- zlepšení cash flow
- poskytnutí alternativní metody placení
- rozšířené nabídky produktů, jako je např. služba DCC

Global Payments s Vámi bude úzce spolupracovat při hledání toho správného řešení v oblasti zpracování transakcí platebních kartou pro Vaše podnikání a představujícího kvalitní službu za co nejvýhodnější cenu pro Vás.

Pokud se v oblasti zpracování transakcí platební kartou rozhodnete pro služby společnosti Global Payments, budeme se neustále snažit o snižování Vašich nákladů, o rozvoj té části Vašeho podnikání, která využívá právě naše služby, snižování či minimalizaci počtu případů, kdy je nutné vrátit peníze za reklamovanou transakci (tzv. chargeback), a minimalizaci dalších poplatků.

TYPY TRANSAKCÍ

Služby v oblasti merchant acquiringu – akceptace a zpracování transakcí uskutečněných platební kartou Vám umožňují přijímat tyto formy plateb od zákazníků a lze je rozdělit na dvě základní skupiny podle typu transakcí:

Transakce, kdy je karta přítomna (CP, Card Present), což znamená všechny transakce, kde jsou karta a její držitel fyzicky přítomni v okamžiku transakce a kde se můžete o přítomnosti karty přesvědčit načtením čipu, protažením magnetického proužku karty čtečkou nebo přiložením k elektronickému terminálu. Zahrnuje následující typy transakcí:

- prodejní transakce týkající se prodeje zboží nebo služeb
- nákup s vrácením hotovosti („cashback“, možný pouze u debetních karet) – transakce spojené s prodejem zboží nebo služeb, kdy zákazník zároveň dostává zpět hotovost

Transakce bez přítomnosti platební karty (CNP, Card Not Present), což znamená transakce, kdy karta a držitel karty nejsou fyzicky přítomni v okamžiku transakce.

Tato skupina zahrnuje následující typy transakcí:

- prodejní transakce s objednávkou přes poštu, telefonicky či pomocí jiného podobného typu komunikace
- transakce uskutečněné přes internet
- opakované transakce (pouze u určitých typů karet), kdy Vás držitel karty oprávní ke strhávání fixních či měnících se částek v určitých časových intervalech (které mohou být předem specifikovány) ze své karty a kam patří předplatné, obnovy členství a pravidelné platby

Existují další typy transakcí, které mohou být buď typu CP nebo CNP, například transakce v několika měnách, přičemž tento manuál pro obchodníky Vám poskytne návod, jak tyto, stejně jako výše zmíněné platby, přijímat.

V Žádosti o akceptaci platebních karet (dále jen „Žádost“) naleznete detailní popis typů transakcí a typů karet, které máte oprávnění přijímat. Ke zpracovávání jiných typů transakcí či k přijímání jiných typů karet, než které jsou uvedené ve Vaší Žádosti, musíte mít naše písemné oprávnění.

POVĚDOMÍ O RIZICICÍH

Naším přáním je, aby Váš podnik mohl přijímat karty bez jakýchkoliv problémů. Je nicméně velmi důležité, abyste si byli vědomi a porozuměli rizikům spojeným s přijímáním karet.

Jedním z těchto rizik je tzv. chargeback (vrácení částky transakce na kartu zákazníka), což je reklamovaná karetní transakce, která nám byla vrácena vydavatelem karty. Je možné, že Vám reklamovanou částku strhneme z Vašeho účtu – tato sekce nicméně popisuje některé způsoby, jak můžete minimalizovat toto riziko pro Vaše podnikání.

Neexistuje žádná záruka proplacení jakékoliv transakce, i když jste obdrželi autorizaci. Autorizace ověřuje, že v okamžiku transakce není karta hlášena jako ztracená či odcizená a že skutečný držitel karty má k provedení transakce k dispozici dostatečné finanční prostředky.

Nikdy nepřipusťte, aby byla hodnota nákupu zaplacena více jak jednou platební kartou, a nikdy nedělte prodejní transakci na více menších částek.

Transakce, kdy je karta přítomna (CP Transakce)

Čipová karta požadující PIN

Transakce vykonaná čipovou kartou požadující PIN v současnosti představuje jednu z nejbezpečnějších metod platby platební kartou. Veškeré CP transakce, při nichž zákazník hodlá platit čipovou kartou s PIN, musí být provedeny s pomocí terminálu, který umožňuje načtení čipu a zadání PIN.

Po vložení čipové karty do terminálu se na platebním terminálu či PIN padu zobrazí částka transakce, držitel karty je vyzván k potvrzení částky zadáním PINu případně může být držitel vyzván nejprve k potvrzení částky a následnému zadání PINu.

V případě, že Váš elektronický terminál není schopen údaje zaznamenané v čipu přečíst, budete muset provést ověření přes magnetický proužek na kartě.

Čipová karta požadující podpis

Existují i čipové karty, které v případě jejich vložení do terminálu namísto zadání PIN požadují podpis držitele karty. V takovémto případě platební terminál vytiskne stvrzenku s řádkem určeným pro podpis držitele karty. Dále postupujte dle pokynů na platebním terminálu.

Bezkontaktní transakce

Váš terminál je vybaven čtečkou pro akceptaci bezkontaktních plateb. Na platebním terminálu či PIN padu se zobrazí částka transakce a držitel karty jednoduše přiloží kartu ke čtečce, čímž bude provedena platba. Pokud s kartou nebo eventuálně s terminálem není možné provádět bezkontaktní platby či pokud držitel karty dává přednost načtení čipu a zadání PIN, pak je možné transakci dokončit vložením karty do čtečky a zadáním PIN.

V některých případech Váš terminál může vyžadovat, aby byla provedena transakce se zadáním PIN namísto transakce bezkontaktní. Jde o dodatečnou bezpečnostní funkci, jejímž cílem je potvrdit, že držitel karty je vlastníkem karty. V tomto případě je třeba pokračovat s načtením čipu karty a zadáním PIN obvyklou cestou.

Transakce s magnetickým proužkem

V oběhu je stále řada platných karet, které neobsahují čip a je třeba je protáhnout čtečkou a načíst data z magnetického proužku.
V případě, že je transakce prováděna přes magnetický proužek v důsledku problémů s čipem, je třeba dbát zvýšené pozornosti, neboť s čipem mohlo být záměrně manipulováno, aby nemuselo dojít k ověření přes PIN.

V těchto případech bude transakce autorizovaná online a na Vás bude, abyste důkladně zkontrolovali, že podpis na účtence se shoduje s podpisem na kartě. Postupujte prosím podle instrukcí uvedených na straně 13 (Kontrola karet). Rovněž je třeba bezpečně si uchovat kopii podepsané účtenky.

Transakce zadávané pomocí klávesnici na terminálu

Pro tuto možnost je potřeba mít na terminálu aktivovanou funkci „Ruční vstup“. V opačném případě není možné provádět ruční zadání čísla karty. Pokud máte zájem o aktivaci této služby, kontaktujte prosím náš helpdesk.

Při provádění tohoto typu transakce postupujte dle pokynů uvedených v Uživatelské příručce pro Váš platební terminál.

CNP transakce

Tyto situace jsou ideální pro podvodníky, neboť platební karta, podpis a osobní identifikační číslo (PIN) nemohou být ověřeny, protože jde o situaci, kdy Vy, karta a držitel karty nejste společně přítomní. Většina reklamovaných transakcí (chargebacks) se týká transakcí, které byly provedeny podvodně. Pokud dokončíte transakci, o níž máte pochybnosti, činíte tak na své vlastní riziko.

Abyste minimalizovali rizika spojená s CNP transakcemi:

- Zvýšené opatrnosti dbejte tehdy, když objednávka přišla z emailového účtu, v němž není zákazníkovo jméno nějakým způsobem obsaženo v emailové adrese.

- Buďte podezřívaví vůči transakcím, které jsou vzhledem k typu Vašeho podnikání nezvykle vysoké co do hodnoty a objemu, případně je prodej „příliš snadný“. Naše zkušenosti nám říkají, že právě u těchto transakcí je zvýšená pravděpodobnost, že budou podvodné.

- Pokud vracíte peníze, vždy je vraťte na stejnou platební kartu, s níž byla provedena původní transakce.

- Veďte si databázi reklamovaných transakcí (chargebacks), abyste mohli snáze odhalit vzorce v podvodných transakcích. Pokud se prodej zdá být „příliš dobrý na to, aby byl skutečný“, pak zřejmě skutečný není. Nebojte se kontaktovat držitele karty, abyste mu položili doplňující otázky či si vyžádali dodatečnou identifikaci. Poctivý zákazník by měl ocenit, že Vám jde o bezpečnost a že se snažíte své zákazníky ochránit před podvody.

- Pro transakce v rámci internetových obchodů by měla být na internetových stránkách implementována ještě další úroveň zabezpečení. Funkce Mastercard SecureCode a Verified by Visa (VbV) byly vytvořeny, aby umožnily se zákazníkům prokázat jako skutečný držitel karty.

- Zboží vždy odesílejte doporučenou nebo zvláštní poštou či prostřednictvím důvěryhodného a bezpečného dopravce. Trvejte na tom, že musí být vystaven doklad o doručení, který musí být následně podepsán, pokud možno držitelem karty. Požádejte kurýra, aby zásilku nedoručil, pokud se prostory, kam má být doručena, zdají prázdné. Mějte prosím na paměti, že doklad o zaplacení jako takový není dostatečným důkazem, který by Vás ochránil před reklamovanou transakcí (chargeback).

- Nikdy nepředávejte zboží třetím stranám, jako jsou například řidiči taxi nebo messengeři.

- Dbejte zvýšené opatrnosti u transakcí, kde je fakturační adresa odlišná od požadované doručovací adresy. Vyhněte se doručování na adresy, které jsou odlišné od adresy držitele karty, jako jsou například hotely, internetové kavárny a adresy jiných osob, u nichž se adresát zdržuje.

- Opatrně postupujte u požadavků na dodání do druhého dne, požadavků na rychlou změnu doručovací adresy a u telefonátů v den doručení, v nichž kupující požaduje určitý čas doručení.

- Pokud zákazník vyžaduje vyzvednutí zboží v obchodě, transakci proveďte při vyzvednutí zboží pomocí Vašeho zařízení, které máte na prodejním místě.

Více informací o tom, jak ochránit Vaše podnikání, naleznete na straně 50.
Pokud byla transakce označena jako podvodná a chargeback byl uznán, budete muset vrátit zaplacenou částku zpět na kartu zákazníka. Může se tedy stát, že Vám hodnotu transakce odepíšeme z účtu. V případě jakéhokoliv podezření zavolejte náš helpdesk a jako důvod autorizace ohlaste „kód 10“ (viz strana 22).

Pamatujte, že autorizace není zárukou platby.

Kopie prodejního dokladu

Kdykoliv si můžeme vyžádat kopie prodejních dokladů. Na jakoukoliv takovou žádost prosím reagujte bez zbytečného prodlení, neboť v opačném případě může dojít k chargebacku. Kopie prodejních dokladů vždy bezpečně uchovávejte v rámci své vlastní evidence. Mějte prosím na paměti, že byste měli uchovávat veškeré doklady o transakcích po dobu pěti let od doručení zboží či dokončení poskytované služby (viz str. 44 pro podrobnější informace o bezpečnosti dat).

Bezpečnost dat

V současné době narůstají obavy o bezpečnost dat. Zločinci hledají nové cesty, jak tyto informace získat z různých zdrojů. Jednou zranitelnou oblastí, kterou se podvodníkům podařilo najít, jsou finanční údaje z platebních karet, které jsou shromažďovány v průběhu zpracování transakcí. Provozovatelé sítí platebních karet zavedli standard s názvem the Payment Card Industry Security Standard (PCI DSS), který představuje globálně závazný standard s cílem zvýšit zabezpečení tohoto typu dat.

Při přijímání transakcí prováděných platební kartou je třeba, abyste si uvědomovali hodnotu dat, která od zákazníka sbíráte, když transakci provádíte, a stejně tak potřebu tyto data chránit. Pokud by došlo k bezpečnostnímu incidentu, vystavujete se tím významnému riziku finančních ztrát a poškození dobré pověsti Vašeho podniku.

U obchodníků přijímajících CNP transakce se požaduje, aby dosáhli souladu se standardy PCI DSS a tento standard nadále dodržovali, a to z důvodu zvýšeného rizika porušení, krádeže či zneužití dat v prostředí CNP.

Více informací o PCI DSS naleznete na str. 44, případně můžete navštívit stránku www.pcisecuritystandards.org, na níž je k dispozici nejnov ější verze standardu PCI DSS a návod na to, jak zajistit soulad s tímto standardem. Informace v českém jazyce naleznete na internetových stránkách Sdružení pro bankovní karty – www.pcistandard.cz.

Zpracování transakcí třetích stran

Zpracovávání transakcí ve prospěch jiného podniku Vám může způsobit výrazné finanční škody. Ať už je Vám nabídnuta paušální platba, za kterou poskytnete neomezený přístup a využívání Vašeho zařízení na zpracovávání plateb kartou, či provize z každé platby, kterou zpracujete, mějte na paměti, že se jen zřídkakdy stává, že tato třetí strana skutečně poskytne slibované služby. Tyto entity, ačkoliv se zdají být poctivými subjekty a udávají zdánlivě věrohodné důvody, proč potřebují Vaši asistenci, jsou jen prázdné schránky, které jsou využívány gangy organizovaných zločinců páchajících podvody např. s prodejem ubytování či lístků.

Nikdy nepřijímejte takové transakce. Podobné transakce jsou většinou napadeny ze strany zákazníka nebo se jedná o transakce podvodné a mohou mít za následek chargeback či finanční ztrátu pro Vaše podnikání. Nastane-li takový případ, budete plně zodpovídat za finanční kompenzaci držitele karty, jemuž nebylo dodáno zakoupené zboží a služba.

Zpracování transakcí třetích stran rovněž porušuje naši Smlouvu o zpracování platebních transakcí kartou a odhalení takové aktivity může mít za následek okamžité ukončení našeho smluvního vztahu. Výše zmíněný typ zpracování transakcí může rovněž vést k trestnímu stíhání.

Terminály

Jste zodpovědní za zařízení terminálu, a proto důrazně doporučujeme, abyste věnovali náležitou pozornost jeho umístění a pravidelné kontrole tohoto zařízení. Zodpovídáte rovněž za veškeré ztráty, které budou způsobeny zásahem třetích osob, které nejsou oprávněny manipulovat se zařízením jiným způsobem, než je běžný průběh transakce, tj. například zadávání PIN.

Zajistěte, že žádné bezpečnostní zařízení (např. bezpečnostní kamera) není schopno pořídit záznam držitele karty při tom, když zadává své PIN.

TRANSAKCE, KDE JE KARTA PŘÍTOMNA (CP)

Transakce „karta přítomna“ (CP) jsou jakékoliv transakce, kde jsou karta a držitel karty fyzicky přítomni spolu s Vámi po celý průběh transakce a kde se můžete přesvědčit o přítomnosti karty, s níž je zadávána transakce do elektronického terminálu.

CP transakce mohou být přijímány a ověřovány řadou způsobů:

- Čipem a PIN
- Čipem a podpisem
- Bezkontaktně
- Magnetickým proužkem a PIN
- Magnetickým proužkem a podpisem
- Ručním vstupem (máte-li tuto funkci povolenou)

Na Vašem terminálu se budou objevovat instrukce, které Vám řeknou, jak máte postupovat. Podrobnější informace o použití Vašeho platebního terminálu naleznete v Uživatelské příručce k Vašemu platebnímu terminálu, která je k dispozici ke stažení na Merchant Portálu.

OVĚŘENÍ DRŽITELE KARTY POMOCÍ PIN

V závislosti na typu terminálu buď Vy, nebo držitel karty vložíte kartu do čtečky karet terminálu či externího PIN padu.

Požadavek provést fyzické či vizuální ověřovací kontroly karty závisí na tom, zda kdykoliv v průběhu transakce s kartou skutečně manipulujete. Pokud s kartou manipulujete, pak musíte postupovat, tak jak je uvedeno v kapitole „Kontrola karet“ na straně 13. Není třeba získat od zákazníka jeho podpis na účtence či dokladu vytištěném terminálem.

OVĚŘENÍ DRŽITELE KARTY PODPISEM

Existují jisté okolnosti, za kterých nemůže být identita držitele karty ověřena prostřednictvím PIN. Tyto okolnosti zahrnují:

- kartu bez čipu (například kartu s magnetickým proužkem)
- čipovou kartu, která nepoužívá jako metodu ověření PIN.

V těchto případech nebude držitel karty vyzván, aby zadal PIN, a namísto toho musí dojít k ověření držitele karty jeho podpisem. Vzhledem k tomu, že budete s kartou manipulovat, bude od Vás vyžadováno provedení fyzické a vizuální kontroly tak, jak je popsáno v kapitole „Kontrola karet“ na straně 13.

OVĚŘENÍ DRŽITELE KARTY PROSTŘEDNICTVÍM PIN A PODPISU

Existují určité typy karet, které, i když jde o karty s magnetickým proužkem vyžadující ověření podpisem, mohou vyžadovat k ověření rovněž PIN. Například karty UnionPay jsou karty s magnetickým proužkem, ale ve většině případů vyžadují rovněž zadání online šestimístného PIN a podpis.

BEZKONTAKTNÍ PLATBY KARTOU

Bezkontaktní platby kartou umožňují provádění transakcí s nízkou částkou, aniž by musela být karta vložena do čtečky či protažena čtečkou magnetického proužku. Pro zpracování těchto plateb je vyžadována bezkontaktní čtečka, která je integrována do Vašeho platebního terminálu.

Do karty je vložena speciální technologie, která ji umožňuje fungovat v bezkontaktním prostředí. Běžné karty s magnetickým proužkem nebo čipové karty se zadáváním PIN nebudou s bezkontaktní čtečkou fungovat. Obecně platí, že když je na přední či zadní straně karty zobrazen následující symbol, pak karta využívá bezkontaktní technologii.

Ačkoliv pro provedení bezkontaktní platby, jejíž výše je pod limitem pro bezkontaktní platby, tzn. že se jedná o transakci do 500,– CZK, není vyžadováno PIN, může se občas stát, že Váš terminál bude požadovat provedení transakce se zadáním PIN namísto transakce bezkontaktní. Jde o dodatečnou bezpečnostní funkci, jejímž cílem je potvrdit, že držitel karty kartu skutečně vlastní – v takovém případě musíte dále postupovat jako u transakce s načtením čipu a zadáním PIN.

Bezkontaktní technologie může být rovněž integrována do dalších zařízení, například do chytrých hodinek, náramků, chytrých telefonů, tabletů a elektronických přívěšků na klíče.

KONTROLA KARET

Typ karty určí, jaké kontroly je třeba provést.

Jak provést kontrolu platební karty

Existuje řada odlišných typů kreditních a debetních karet. Popis kontrol uvedený níže se vztahuje na většinu karet vydávaných bankami či jinými finančními institucemi. V případě, že neprovedete tyto kontroly, může být proti Vám uplatněn chargeback:

1. Čip

- Pokud je na kartě čip, zkontrolujte, zda nenese známky pokusu jej odstranit, vyměnit nebo poškodit.

2. Číslo karty

- Číslo účtu držitele karty začíná číslicí 2 nebo 5 pro karty Mastercard, 6 pro Maestro, 4 pro Visa, 36 pro Diners Club, 6011, 64 nebo 65 pro Discover, 62 pro UnionPay[1], 35 pro JCB a 37 pro karty Amex.

- První čtyři číslice čísla účtu se mohou opakovat nad nebo pod začátkem embosovaného čísla karty – zkontrolujte, že se shodují s prvními čtyřmi číslicemi embosovaného čísla, pokud jsou na kartě uvedeny.

- Poslední čtyři číslice čísla karty na přední straně karty se musí shodovat s číslem na zadní straně na podpisovém proužku (v případě, že je na kartě uvedeno) a rovněž s čtyřmi posledními číslicemi čísla karty na účtence vytištěné terminálem.

- U embosovaných karet zkontrolujte čísla. Pokud je oblast kolem nich poškozená, může to znamenat, že původní čísla mohla být odstraněna a nahrazena novými.

- Číslo účtu na přední straně karty mohlo být vytištěno a nikoliv vyraženo, a proto může na dotek působit spíše hladce než vystouple. Nehledě na to, zda jsou karty embosované či ne, u karet Visa Electron, Maestro, V PAY, Discover Global Network a UnionPay nelze provádět platby pomocí imprinteru (a papírových účtenek).

- Pokud je na kartě uvedeno „Electronic Use Only“, transakce nemohou být prováděny pomocí imprinteru a papírových účtenek.

3. Oslovení a jméno držitele karty

- Zkontrolujte, zda mezi držitelem karty a údaji na kartě nejsou zjevné nesrovnalosti, jako když například žena užívá kartu, na které je uvedeno oslovení „Mr.“, nebo když teenager používá kartu s titulem „Doktor“.

- Některé karty obsahují fotografii držitele. Je třeba zkontrolovat, že fotografie odpovídá osobě, která předkládá kartu, a že fotografie nebyla pozměněna.

4. Platná od/vypršení platnosti/platná do

- Kartu je třeba důkladně prohlédnout s ohledem na její platnost. Nepřijímejte karty, které jsou předkládány k provedení transakce před datem „platná od“ (kde je toto datum uvedeno) či po datu vypršení platnosti/platná do. Terminál automaticky provede na kartě určité kontroly, avšak nelze nás činit odpovědnými za to, že terminál přijme kartu, která ještě není platná nebo kartu, jejíž platnost vypršela.

5. Hologram

- Zkontrolujte, zda nenese známky manipulace. Hologram by měl být na dotek hladký a neměl by mít hrubý či poškrábaný povrch a 3D obrázek by se měl při naklonění hýbat. Padělané karty často obsahují nedokonalé napodobeniny hologramů.

- Hologram může být na přední nebo na zadní straně karty, ledaže je na kartě užita Holomag páska (holografická magnetická páska) na místo tradičního magnetického proužku

[1] Karty UnionPay s dvojí značkou začínají také číslicí 3, 4, 5 nebo 9

• Mezi nejčastější podoby hologramů patří:
– Mastercard – obrázek zeměkoule
– Visa – letící holubice nebo několik holubic v letu
– Visa Electron – ne všechny karty obsahují hologram. Pokud se hologram na kartě vyskytuje, vypadá jako letící holubice
– UnionPay - 3D obrázek Chrámu nebeského
– Diners – rozdělený kruh
– JCB – úsvit
– Amex – římský centurion

6. Podpisový proužek

• Pamatujte – pokud je karta ověřována pomocí PIN, není třeba ověřovat, že se podpis shoduje.

• Podpis by měl být napsaný jasně a měl by být hladký na dotek. Buďte podezřívaví, pokud karta není podepsaná. Pokud se zdá, že podpis byl vymazán, pokud se karta zdá být podpis přepsaný či pokud byl podpis napsaný velkými písmeny či byl napsán fixou.

• Zkontrolujte, že podpis odpovídá jménu uvedenému na přední straně karty.

• Zkontrolujte, zda podpisový proužek nenese známky manipulace či zda na něm není vidět pozůstatek po smazaném podpisu.

• Zkontrolujte, že podpis na kartě odpovídá podpisu na účtence vytištěné terminálem

Pokud je Vám předložena nepodepsaná karta, požádejte držitele karty, aby prokázal svou totožnost a podepsal kartu ve Vaší přítomnosti. Zapište druh a číslo průkazu totožnosti na prodejní doklad a autorizujte transakci bez ohledu na výši transakčního limitu.

7. Bezpečnostní kód karty (CSC)/Kontrolní číslice (CVV2)

• Trojmístný nebo čtyřmístný ověřovací kód. U karet Mastercard, Visa a Maestro kód CSC představují tři poslední číslice vytištěné na zadní straně karty za posledními čtyřmi číslicemi čísla účtu držitele karty, pokud jsou tam tyto uvedeny. Kód CSC může být rovněž uveden na samotném podpisovém proužku či v bílém políčku napravo od podpisového proužku. U karet American Express má toto číslo čtyři číslice a je vytištěno na přední straně karty.

8. Magnetický proužek

• Ujistěte se, že karta má magnetický proužek na zadní straně. Pokud je magnetický proužek na dotek nezvykle hrubý nebo poškrábaný, je na místě pojmout podezření, že karta byla padělána.

• Některé karty mají pásku Holomag (holografický magnetický proužek) na místě tradičního magnetického proužku. Pokud je na kartě přítomen pásek Holomag, musí být vždy na zadní straně karty a karta už nesmí obsahovat žádný jiný hologram.

9. Ultrafialové prvky

• Pokud máte UV tester bankovek, můžete provést kontrolu ultrafialového znaku na přední straně karet.

10. Fotografie

• Některé karty obsahují fotografii držitele karty, a to napravo na přední straně karty. Pokud je Vám předložena karta, která obsahuje tento prvek, zkontrolujte, že fotografie odpovídá osobě, která kartu předkládá k provedení transakce. V případě, že mezi fotografií a držitelem není shoda, je oprávněné pojmout podezření.

11. Loga na kartách

• Loga na kartách – objevují se zpravidla na přední straně karty, avšak mohou se objevit i na zadní straně. Měly by být vyvedeny jasně a v ostrých barvách – logo, které je neostré okolo okrajů či které je vyvedeno v nízké kvalitě, může indikovat, že karta byla padělána.

Pokud máte jakékoliv podezření o kartě či o jejím držiteli, kontaktujte telefonicky náš helpdesk a nahlaste „kód 10“ (viz strana 22).

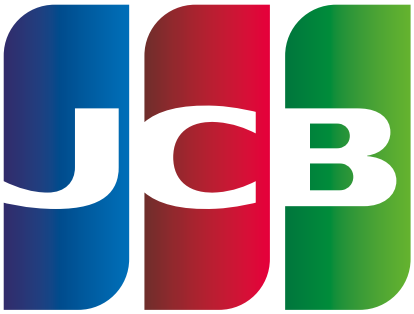
PŘÍKLADY LOG KARET

Discover

Mastercard

UnionPay

Visa



JCB

Diners Club

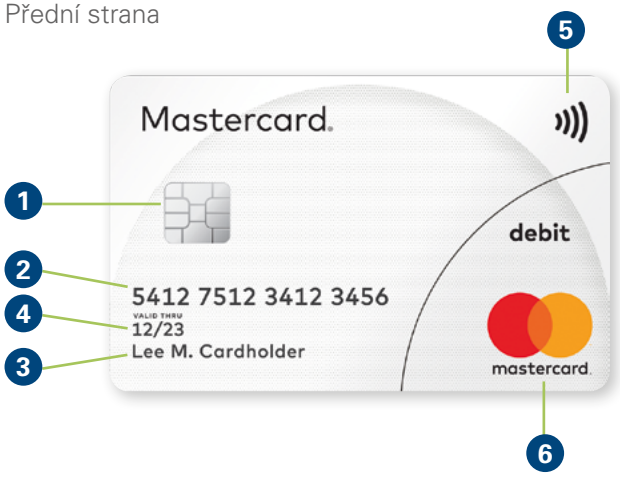
American Express

PŘÍKLADY KARET A PRVKŮ NA KARTÁCH

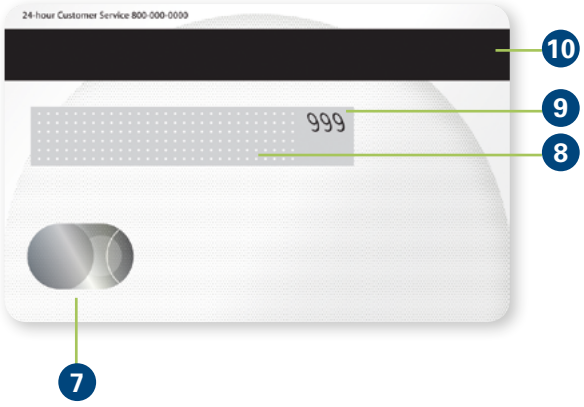
Legenda k obrázkům karet:
1. Čip
2. Číslo karty
3. Titul a jméno držitele karty
4. Platná od/datum vypršení platnosti (popisek „Valid Thru“ uvádí poslední měsíc platnosti)
5. Bezkontaktní logo (pokud je karta obsahuje)
6. Logo karty
7. Hologram
8. Podpisový proužek
9. Bezpečnostní kód karty (CSC)
10. Magnetický proužek/Holomag páska
11. Jiné znaky pro přijímání karty

Mastercard

Přední strana



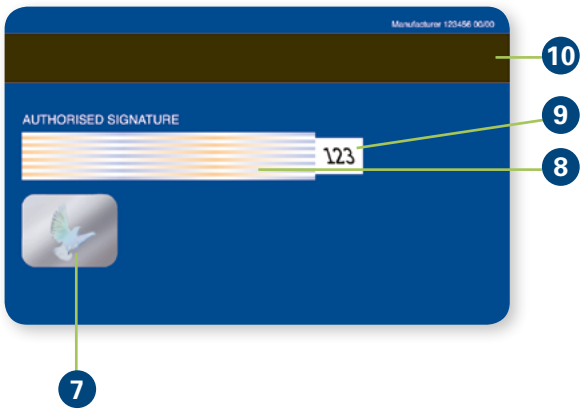
Zadní strana



Visa

Přední strana

Zadní strana



Diners Club International

Přední strana

Zadní strana

Discover

Přední strana

Zadní strana

PŘÍKLADY KARET A PRVKŮ NA KARTÁCH

Legenda k obrázkům karet:
1. Čip
2. Číslo karty
3. Titul a jméno držitele karty
4. Platná od/datum vypršení platnosti (popisek „Valid Thru“ uvádí poslední měsíc platnosti)
5. Bezkontaktní logo (pokud je karta obsahuje)
6. Logo karty
7. Hologram
8. Podpisový proužek
9. Bezpečnostní kód karty (CSC)
10. Magnetický proužek/Holomag páska
11. Jiné znaky pro přijímání karty

UnionPay International

Přední strana

Zadní strana

JCB (Japan Credit Bureau)

Přední strana

Zadní strana

Ve spolupráci s

American Express

Přední strana

Zadní strana

PŘIJÍMÁNÍ KARET PROSTŘEDNICTVÍM PLATEBNÍHO TERMINÁLU

Karty můžete přijímat buď prostřednictvím námi dodaného terminálu či, po vzájemné předchozí dohodě, pomocí Vašeho vlastního zařízení.

Používání námi dodaného terminálu

Než začnete:

- Přečtěte si návod k použití terminálu, neboť v něm nalezete informace o přijímání karet.
- Zkontrolujte, že datum a čas na Vašem terminálu jsou správné. Pokud nejsou správné, proveďte jejich reset na základě instrukcí v návodu k použití terminálu.
- Při umisťování terminálu či PIN padu mějte na paměti jejich dostupnost a soukromí všech držitelů karet, včetně těch s postižením.
- Zajistěte, že budete mít snadný přístup k elektrickým a telefonním zásuvkám u Vašeho karetního terminálu v případě, že nastanou jakékoliv technické problémy a budeme od Vás vyžadovat, abyste v rámci identifikace problému provedl/a určité testy.
- Zajistěte, že žádné bezpečnostní zařízení (jako např. bezpečnostní kamery) není schopno pořídit nahrávku zákazníka zadávajícího PIN.

Prosím konzultujte s námi veškeré změny na Vašem terminálu, včetně jeho výměny, odstranění či přemístění. V případě mobilních terminálů je každodenní přemisťování povoleno v rámci jejich běžného užívání.

V případě, že potřebujete jakoukoliv pomoc, nám prosím zavolejte (viz str. 54, kde jsou uvedeny naše kontaktní údaje).

Používání vlastního zařízení

Služby zpracování transakcí poskytujeme rovněž podnikům, které přijímají platební karty pomocí vlastního zařízení či systému přijímání karet (včetně jakékoliv části tohoto zařízení poskytnutého třetí stranou).

Jsme schopni podporovat oba dva hlavní systémy přijímání platebních karet, jimiž jsou:

- systémy elektronického pokladního místa (EPOS) schopné přijímat karty
- elektronické terminály na přijímání platebních karet, které fungují nezávisle na Vašem pokladním zařízení.

Pro oba tyto systémy Vám můžeme poskytnout:

- systémové specifikace podrobně uvádějící naše požadavky a rozhraní.

Veškeré zařízení musíme před implementací otestovat a schválit. V případě, že užíváte své vlastní zařízení, se musíte řídit všemi procedurami popsanými v tomto návodu, ledaže se nedomluvíme na alternativních a/nebo dodatečných procedurách, které budeme dokumentovat zvlášť.

Je třeba, abyste nás informovali o veškerých navrhovaných změnách týkajících se terminálů, jejich nastavení a přenosových spojeních. Pokud tak neučiníte, může se stát, že nebudeme moci zpracovávat Vaše transakce a vznikne zpoždění v připsání těchto transakcí na Váš bankovní účet.

Pokud využíváte jako poskytovatele třetí strany, musíte nás informovat o jakékoliv změně tohoto poskytovatele. Musíte rovněž zajistit, že poskytovatel dodržuje standardy Payment Card Industry Data Security Standard (PCI DSS, viz str. 44)

Vaší odpovědností je zajistit, že Vaše zařízení pro akceptaci platebních karet splňuje bezpečnostní standardy obvyklé pro dané odvětví. Musíte provádět a hradit náklady za veškerý upgrade Vašeho zařízení, který můžeme my nebo dodavatel Vašeho terminálu v případě potřeby vyžadovat. Výše uvedené zahrnuje veškerá vylepšení, která je třeba provést, aby Vaše zařízení odpovídalo změnám v pravidlech provozovatele. Neschopnost na tyto změny reagovat může způsobit nesoulad s výše zmíněnými nařízeními a může mít za následek poplatky a pokuty a zvýšené riziko chargebacků.

AUTORIZACE

Proces zpracování transakce je vždy dán konkrétním nastavením poskytovatele služeb. Naše společnost podporuje níže popsaný systém.

Online autorizace

Při Online autorizaci je transakce okamžitě odeslána do autorizačního centra. Autorizovaná částka se přičte do terminálových součtů pro kontrolní a administrativní účely. Takto jsou procesovány veškeré transakce bankovními kartami, vyjma transakcí popsanými v části Offline autorizace.

Offline autorizace

Při Offline autorizaci je transakce autorizována v terminálu. Takto jsou autorizovány transakce provedené bezkontaktními i kontaktními kartami, jejich hodnota a počet je individuálně posuzována a schválena bankou, která vám terminál dodala.

Semi-offline autorizace

Při Semi-offline autorizaci je transakce autorizována v terminálu a po dokončení transakce je na pozadí tisku stvrzenek odesílána do autorizačního centra k dalšímu zpracování.

Pokud byla transakce přijata, dle nastavení terminálu se data buď okamžitě odesílají, nebo se ukládají v terminálu a musí být odeslána v rámci dávky do autorizačního centra.

Autorizace na POS terminálu je zajištěna automaticky pokud částka prodeje překročí autorizační limit.

Autorizace neprovádí potvrzení identity držitele karty a není ani garancí platby.

Pokud máte jakékoliv podezření o kartě či o jejím držiteli, kontaktujte telefonicky náš helpdesk a nahlaste „kód 10“ (viz strana 22).

Předautorizace

Předautorizace se používá převážně v oblasti cestovního ruchu, zejména v ubytovacích zařízeních a půjčovnách, kde konečná částka transakce nemusí být známa v okamžiku původní autorizace. Předautorizace je proces, při kterém dochází u obchodníka k ověření platnosti platební karty a dostatečnosti finančního krytí na účtu držitele platební karty pro předpokládanou platební transakci.

Předautorizaci lze provádět pouze prostřednictvím elektronického platebního terminálu POS pro všechny typy karet vyjma platebních karet Maestro, Mastercard Electronic, Visa Electron a V PAY. Obchodník je povinen dokončit předautorizaci do 30 dnů od data zahájení předautorizace.

Částka předautorizace musí vždy odpovídat předem dohodnuté ceně služby či zboží mezi obchodníkem a držitelem karty. Držitel karty musí být předem informován o předautorizaci a musí s ní souhlasit.

Postupy, jak vykonat transakci „Předautorizace“, jsou popsány v Uživatelské příručce pro platební terminál.

Zakončení předautorizace

Transakce zakončení předautorizace je prakticky dokončením prodeje, který byl dříve předautorizován. Částka zakončení předautorizace se může lišit od částky zadané při předautorizaci. Zakončení předautorizace může být rovněž provedeno i v nepřítomnosti držitele karty. Tento typ transakce lze provést s využitím magnetických, čipových a rovněž bezkontaktních karet.

Ve chvíli, kdy chcete dokončit předautorizaci, musíte mít připravený 6 místný autorizační kód a 9 místný identifikátor z účtenky předautorizace. Rovněž musíte znát skutečnou částku pro zakončení předautorizace.

Při zakončení předautorizace na Vašem platebním terminálu postupujte přesně podle pokynů uvedených v Uživatelské příručce.

Storno libovolné transakce

Transakce storno slouží ke zrušení jakékoliv transakce, jejíž stáří nepřekročilo 95 dnů. Transakci lze stornovat na libovolném terminálu v rámci jednoho obchodního místa (provozovny). Částku lze stornovat v plné výši transakce nebo jen částečně. Pokud bylo u stornované transakce využito služby DCC, je možné zrušit pouze celou transakci a částka ke stornování je zadávána v CZK.

Detailní postup storna transakce je popsán v Uživatelské příručce pro Váš platební terminál.

Jaké autorizační hlášky se budou objevovat na mém terminálu?

Ve chvíli, kdy byla automaticky vygenerována žádost o autorizaci, zobrazí terminál v odpovědi na požadavek hlášku. Mohou se objevit následující typy hlášek:

PRIJATO
Autorizace proběhla úspěšně. Transakce povolena.

PRIJATO – OVERTE TOTOZNOST
„autor- kód xxxxxx"
Transakce je přijata a identita držitele karty musí být ověřena. Na stvrzenku napište číslo a typ dokladu totožnosti.

„VOLEJTE AC", „VOLEJTE HLAS. AUT."
Pokud se na Vašem terminálu objeví jedna z těchto zpráv ve chvíli, kdy se snažíte získat automatickou autorizaci, musíte zavolat náš helpdesk (kontaktní údaje naleznete na str. 54). Tyto zprávy naznačují, že potřebujeme provést dodatečná bezpečnostní ověření, která jsou vyžadována vydavatelem katy. Vždy musíte zavolat na náš helpdesk předtím, než přijmete jiný způsob platby.

„ZAMITNUTO"
Transakce nelze provést. Pokud chcete společně s držitelem karty pokračovat v prodeji, požádejte jej o alternativní způsob platby.

„KARTA NEPOVOLENA"
Zkontrolujte, že máte oprávnění přijímat tento typ karet. Pokud si nejste jisti, měli byste kontaktovat helpdesk (kontaktní údaje naleznete na str. 54). Pokud máte oprávnění přijímat karty předloženého typu, zavolejte prosím náš helpdesk a ohlaste „kód 10" (viz strana 22).

„NEPODPOROVANA KARTA"
Kartu nelze pro daný typ transakce použít. Můžete požádat o alternativní způsob platby.

„ZADRZTE KARTU"
Pokyn zadržet kartu, s kterou je prováděna transakce, byl vydán bankou, která je vydavatelem karty.

„NEPLATNA KARTA"
Doba platnosti karty skončila, anebo bylo chybě zadáno číslo karty při ručním zadávání nebo jsou chybné údaje v magnetickém záznamu. Transakci nelze provést.

„CAS VYCERPAN"
Při zpracování transakce došlo k chybě a systém nevrátil odpověď na autorizační požadavek v časovém limitu.

Pokud Váš terminál není nastaven, aby prováděl autorizaci automaticky, či pokud se na něm vyskytne chyba, která zabraňuje, aby Váš terminál získával autorizace automaticky, je třeba, abyste zavolali na náš helpdesk (kontaktní údaje naleznete na str. 54).

Kdy je třeba provádět hlasovou autorizaci?

Náš helpdesk (kontaktní údaje naleznete str. 54) musíte zavolat v případě, že:

- Nejste schopni získat automatickou autorizaci
- Na displeji terminálu se objeví zpráva „Volejte AC"; „Volejte hlas. aut." nebo „Zadržte kartu"
- Pokud pojmete jakékoliv podezření o předkládané kartě či o jejím držiteli

Hlasová autorizace **neslouží**:

- k potvrzení identity držitele karty a
- jako garance platby

Autorizační limity

Autorizační limity jsou nastaveny provozovatelem sítě kreditních karet. Vydavatel nicméně může nastavit jím preferovaný autorizační limit na kartě, který pak může mít přednost před limitem nastaveným na terminálu.

V případě nutnosti můžeme změnit Váš autorizační limit v rámci naší snahy bojovat s podvody či na žádost provozovatele sítě kreditních karet. O jakékoliv případné změně Vás budeme informovat a poskytneme Vám potřebné instrukce.

TELEFONÁT S NAHLÁŠENÍM „KÓDU 10"

Telefonní hovor s nahlášením „kódu 10" by měl být proveden zavoláním na náš helpdesk (kontaktní údaje jsou uvedeny na str. 54), pokud:

- máte jakékoliv podezření ohledně karty, držitele karty, či okolností transakce

- jste od nás získali pokyn tak učinit jako opatření na prevenci podvodů.

Co potřebujete k telefonátu s nahlášením „Kódu 10“

- číslo obchodníka
- výši transakce zaokrouhlenou na celé koruny; pokud transakce není prováděna v Českých korunách, uveďte měnu a částku
- autorizační kód, pokud byl kód poskytnut s původní transakcí, například spolu s online autorizací
- bude třeba, abyste jasně uvedli, proč máte podezření týkající se karty a/nebo jejího držitele
- měli byste zajistit, že hovor provádíte co nejdiskrétněji
- můžete dostat pokyn, abyste držiteli karty položili z bezpečnostních důvodů řadu otázek

Tyto bezpečnostní kontroly byste měli provést i tehdy, když Vám zákazník nabízí alternativní způsob platby. Je důležité, abyste provedli telefonní hovor s nahlášením „kódu 10“ i tehdy, když Vás zákazník požádá o vrácení karty či když opustí prostory, aniž by byla transakce dokončena.

Nezapomeňte:

- upozornit držitele karty na to, že za okamžik bude provedena rutinní bezpečnostní kontrola nebo že Váš zpracovatel karet si vyžádal rutinní bezpečnostní prověření transakce. Ponechte si kartu i zboží u sebe, dokud bezpečnostní kontroly neproběhnou.
- zatelefonovat na náš helpdesk (kontaktní údaje jsou uvedeny na str. 54)
- získat autorizační kód přímo od nás, a nikoliv od držitele karty či od kohokoliv jiného, jako je například vydavatel karty, který by mohl být v hovoru zapojen
- netelefonujte na žádná telefonní čísla, která Vám dá držitel karty
- neprovádějte telefonát s nahlášením „kódu 10“, pokud se cítíte ohrožení nebo se domníváte, že to není bezpečné, například pokud jste v obchodě sami; v tomto případě nám zavolejte ihned poté, co držitel karty odešel, neboť takový telefonát může pomoci zabránit další podvodné činnosti páchané jinde.

Při zadržení karty byste neměli sebe sama ani své kolegy vystavovat nebezpečí. Pokud se osoba, která předkládá kartu k transakci, začne chovat agresivně nebo násilně, vždy jim kartu vraťte, a to i když jsme Vás požádali o její zadržení.

Pokud stále máte podezření

Poté, co jste provedli hovor s nahlášením „kódu 10“ a získali autorizaci, nejste nijak povinni transakci dokončit. V takovém případě však nesmíte kartu zadržet.

ZADRŽENÉ KARTY

Zadržení karty

Pokud Vás požádáme, abyste kartu zadrželi, pokuste se tak prosím učinit.

Pokud se osoba, která předkládá kartu k transakci, začne chovat agresivně či násilně, vždy jí kartu vraťte, a to i tehdy, když jsme Vás požádali o zadržení karty. V této situaci byste vždy měli:

- pokusit se zaznamenat detaily o vzhledu osoby, která předkládá kartu k transakci, a použít monitorovací zařízení (např. bezpečnostní kameru), pokud máte k dispozici
- zatelefonovat na náš helpdesk (kontaktní údaje jsou uvedeny na str. 54) a vysvětlit nám, že jste nebyli schopni kartu zadržet, jak jste o to byli požádáni.

Za určitých okolností budeme kontaktovat policii. Pokud policie o kartu požádá:

- předejte kartu policii
- zaznamenejte si jméno policisty, jeho identifikační číslo a telefonní číslo policejní stanice
- oznamte vyšetřujícímu policistovi, zda jste použili bezpečnostní kameru, a případnou videonahrávku

s důkazním materiálem uchovejte po dobu nejméně 30 dní

Pokud dojde k zadržení karty:

- ihned vyplňte Formulář o zadržení karty
- poskytněte co nejvíce informací o osobě, která předkládala kartu k transakci, a další relevantní informace, jako je například státní poznávací značka jejího vozidla
- kartu do poloviny podélně přestřihněte tak, aby podpisový proužek, magnetický proužek, embosované číslo karty, hologram a čip zůstaly neporušeny
- okamžitě nám předejte obě části karty a vyplněný Formulář o zadržení karty
- uschovejte si kopii Formuláře o zadržení karty

Global Payments s.r.o.
V Olšinách 80/626
100 00 Praha 10 – Strašnice
Česká Republika

Nález karty či karta zapomenutá v prostorách Vaší provozovny

Uchovejte prosím veškeré karty zapomenuté zákazníky na bezpečném místě (např. trezor dle standardu PCI DSS) po dobu 24 hodin.

Pokud se zákazník o kartu přihlásí, nepředávejte mu kartu, dokud jste si neověřili identitu držitele karty:

- požádejte o dostatečný průkaz totožnosti, jako je například řidičský průkaz
- ověřte podpis na kartě vůči ukázkovému podpisu osoby, která se o kartu přihlásila
- pokud máte pochybnosti, kontaktujte náš helpdesk (kontaktní údaje jsou uvedeny na str. 54).

Pokud se o kartu nikdo nepřihlásí do 24 hodin:

- kartu do poloviny podélně přestřihněte tak, aby podpisový proužek, magnetický proužek, vyražené číslo karty a čip zůstaly neporušeny.
- Vyplňte formulář o zadržení karty
- Zašlete obě části karty spolu s Formulářem o zadržení karty na adresu uvedenou výše.

VRÁCENÍ PENĚZ

Peníze mohou být vráceny pouze na stejnou kartu, jaká byla použita při původní prodejní transakci.

- Vrácená částka nesmí překročit částku původní transakce.
- Nikdy nevracejte peníze jiným způsobem a nepřistupujte na možnost vrácení peněz hotově či převodem na bankovní účet atd.

Zrušení transakce

Pokud se držitel karty rozhodne, že zboží nebo služby nezakoupí, musíte transakci zrušit. Kroky, které musíte provést, závisí na tom, jak jste kartu přijali, a na fázi, v jaké se nacházela transakce v momentě, kdy se držitel karty rozhodl ji zrušit.

Pokud jste nedokončili transakci:

- Ověřovanou PIN – můžete zrušit transakci, když na klávesnici terminálu zadáváte částku. Případně může transakci zrušit držitel karty při zadávání PIN.
- Ověřovanou podpisem – můžete zrušit transakci ve chvíli, kdy Vás terminál vyzve k potvrzení podpisu držitele karty.
- Zrušení jakékoliv transakce, jejíž stáří nepřekročilo 95 dnů – viz uživatelská příručka k Vašemu terminálu.

Jakmile je zrušení provedeno, měli byste držiteli karty poskytnout kopii dokladu potvrzujícího zrušení.

Zpracování transakcí

Nabízíme zúčtování probíhající 7 dnů v týdnu. Systémová lhůta pro zúčtování je ve 22:55. Veškeré transakce předložené ke zúčtování před touto lhůtou budou odeslány z našeho účtu na Váš účet následující den, tedy D[2]+1. Veškeré transakce uskutečněné po této systémové lhůtě budou odeslány z našeho účtu 2. následující den, tedy D+2.

[2)] D… den uskutečnění transakce

IMPRINTER A POUŽITÍ PAPÍROVÝCH PRODEJNÍCH DOKLADŮ

Naše společnost nepodporuje možnost využívání imprinterů a nelze je tudíž používat jako záložní řešení akceptace platebních karet. Prodejní doklady vytvořené prostřednictvím imprinteru nebudeme akceptovat k dalšímu zpracování.

TRANSAKCE BEZ PŘÍTOMNOSTI PLATEBNÍ KARTY (CNP)

Transakce, kde je karta nepřítomna (CNP), jsou jakékoliv transakce, kde karta a držitel karty nejsou s Vámi v okamžiku transakce fyzicky přítomni.

Tyto transakce představují příležitost pro podvody, neboť nelze zkontrolovat kartu, podpis a osobní identifikační číslo (PIN).

MO/TO – PŘIJÍMÁNÍ TELEFONICKÝCH OBJEDNÁVEK A OBJEDNÁVEK POŠTOU

MO/TO je transakce provedená na základě písemné či telefonické objednávky zboží či služeb a souhlasu držitele karty. Platba je následně provedena bez fyzického předložení karty jejím, držitelem vůči poskytovateli zboží či služeb, tj. obchodníkovi.

Transakce MO/TO lze provádět, pouze na platebním terminálu a pouze pokud máte s námi písemně uzavřenou smlouvu na akceptaci tohoto typu transakcí.

Pokud přijímáte MO/TO transakce, musíte zajistit, že Vám držitel karty poskytne následující informace:

- typ karty
- bezpečnostní kód karty (CSV)
- číslo karty
- jméno a iniciály přesně tak, jak jsou uvedeny na kartě
- datum začátku platnosti (pokud je na kartě uvedeno)
- datum expirace
- jméno na výpisu z karty
- adresu na výpisu z karty
- kontaktní telefonní číslo

Držitele karty musíte informovat o celkové hodnotě transakce (včetně měny) a získat od nich písemný souhlas strhnout tuto částku z jeho karty.

Musíte rovněž zajistit, že:

- všechny písemné objednávky obsahují podpis držitele karty
- zavedete proces, pomocí něhož budete kontrolovat, zda se různé transakce vztahují k jedné a téže adrese nebo zda je to samé číslo karty používáno pro různé adresy

Při zrušení objednávky provádějte refundaci vždy pouze na platební kartu, která byla použita k provedení původní transakce. Nikdy nevracejte peníze jiným způsobem.

Provedení transkace MO/TO na Vašem platebním terminálu

Transakci lze provést pouze ručním zadáním čísla karty. Tento typ transakce je vždy posílán k online autorizaci. Obchodník si na svém terminálu zvolí funkci MENU – Transakce – MOTO a dále pokračuje dle pokynů na platebním terminálu.

Podrobný návod jak provést tento typ transakce naleznete v Uživatelské příručce Vašeho terminálu.

GP WEBPAY

GP webpay je internetová platební brána pro rychlé a bezpečné platby kartou vytvořená naším servisním partnerem - společností Global Payments Europe, s.r.o. Tato služba umožňuje internetovým obchodům přijímat platby prováděné platebními kartami Visa, Mastercard a Diners Club. Rovněž podporuje platby prostřednictvím digitálních peněženek Masterpass a MasterCard Mobile. GP webpay plně podporuje 3D Secure standard.

Hlavní výhody GP webpay v kostce:

– Přijímat platby 3D Secure – karty vydané asociacemi Mastercard a Visa

– Přijímat platby SSL – karty vydané asociací Diners Club a opakované platby

– Přijímat platby s využitím digitální peněženky – Masterpass a MasterCard Mobile

– Přijímat platby s využitím platebního tlačítka – PLATBA 24 (platební tlačítko Internet bankingu SERVIS 24 poskytovaného Českou spořitelnou, a.s.)

– Využívat funkce usnadňující platby – Opakovaná platba, Fastpay, PUSH platba

– Využívat intuitivní a responsivní design platební stránky

– Využívat ve spolupráci s poskytovatelem funkce pro omezení podvodů – Fraud Prevention System

– Využívat rozhraní API HTTP a API WS (Web Services) pro integraci s eshopem

– Využívat portál GP webpay – správa plateb, uživatelů a klíčů, stažení technické dokumentace a dalších zdrojů pro integraci s rozhraním platební brány GP webpay

– Konzultace a podpora poskytovaná týmem odborníků při zavádění tohoto řešení a při jeho provozu

Zabezpečení plateb

– GP webpay dodržuje mezinárodní standardy a splňuje nejpřísnější bezpečnostní požadavky Mastercard SecureCode, Verified by Visa a SafeKey, stanovené karetními asociacemi Mastercard a Visa. Tyto standardy jsou označeny jako 3D Secure a zajišťují maximální bezpečnost platby.

– PCI DSS představuje soubor bezpečnostních standardů, jehož cílem je zamezit jakémukoliv úniku údajů o držitelích karet. Již řadu let podstupujeme kontroly prováděné nezávislým mezinárodním auditorem, který důkladně zkoumá naši schopnost chránit citlivá data.

Pokud si přejete dozvědět více o GP webpay, neváhejte nás kontaktovat (kontaktní údaje jsou uvedené na str. 54)

OPAKOVANÁ PLATBA

Funkce opakovaná platba je definovaná asociacemi jako karta platbou související s opakující se fakturací s předem určenými a zákazníkem odsouhlasenými podmínkami, jako je např. pevné datum nebo pevná částka.

Porozumění rizikům

- Jakákoliv opakovaná platba zpracovaná poté, co držitel karty zrušil oprávnění k platbě, bude mít za následek chargeback.

- Opakované transakce neposkytují žádnou záruku definitivního obdržení platby a podnikáte je na vlastní riziko.

- Pokud držitel karty vznese stížnost vůči transakci, nesmíte žádné další transakce zpracovávat.

Jak vytvořit souhlas s dohodou o opakující se platbě

Před zpracováním první opakované transakce musíte mít předchozí písemný souhlas držitele karty s prováděním opakované platby. Za tímto účelem Vám doporučujeme připravit si návrh Smlouvy o opakované platbě (Recurring Transaction Agreement, RTA).

RTA musí obsahovat:

- Částku a datum

- Zda je částka/datum fixní nebo variabilní

- Způsob komunikace se zákazníkem

Povinností obchodníka je:

- potvrdit RTA zákazníkovi do dvou dnů dohodnutým způsobem komunikace

- RTA musí být uchována po dobu trvání smlouvy a poskytnuta na žádost vydavatele karty (emailem či v jiném elektronickém formátu, případně v papírové podobě).

Rovněž prosím zajistěte, že:

- u předem nespecifikovaných částek je držitel karty písemně informován o přesné výši částky alespoň 14 dní před tím, než je každá částka účtována

- uchováte písemné/emailem učiněné oprávnění držitele karty po dobu pěti let od data poslední platby nebo od zrušení oprávnění (viz str. 44)
- informujete zákazníka o tom, že mohou kdykoliv dohodu zrušit a sdělíte mu, jak Vám má oznámit zrušení
- na žádost o zrušení budete rychle reagovat
- údaje z karty jsou bezpečně uschovány a neobsahují CSC držitele karty.

Jak provádět opakující se transakce

První tzv. registrační platba probíhá jako standardní platba 3D Secure a musí při ní dojít k ověření držitele platební karty a k zaplacení. V případě zamítnutí platby nelze pod daným RTA provádět další platby a obchodník musí informovat zákazníka.

V případě, že obchodník nabízí bezplatné zkušební období, musí být zákazník informován 7 dní předem o provedení platby na konci tohoto období.

Opakovaná platba probíhá s využitím API WS (Web Services) bez přesměrování prohlížeče zákazníka na platební stránku pro zadání údajů o platební kartě. GP webpay provede rovnou autorizaci platby, která probíhá se zabezpečením SSL bez ověření držitele platební karty.

Obchodník by měl zákazníka upozornit na blížící se konec platnosti jeho karty a nabídnout mu obnovu RTA.

Obchodník musí upozornit zákazníka nejméně sedm pracovních dnů před další opakovanou platbou dohodnutým způsobem komunikace ve všech následujících případech:

- Od poslední platby uplynulo více než šest měsíců
- Skončilo bezplatné zkušební období, úvodní nabídka nebo propagační akce
- V RTA došlo ke změně částky a/nebo data pro opakovanou platbu

Zrušení

Obchodník musí zákazníkovi umožnit jednoduché a snadno dostupné online zrušení opakované platby.

Opakovanou platbu může za zákazníka zrušit také vydavatel jeho karty. V takovém případě je zneplatněna registrační platba a nelze k ní vytvářet opakovanou platbu.

Registrační platba je automaticky zneplatněna, pokud k ní nebyla během jednoho roku vytvořena opakovaná platba, a nelze k ní vytvářet opakovanou platbu.
Vytvoření registrační a opakované platby popisuje technická specifikace pro vývojáře.

Důležité upozornění: opakovanou platbu není možné provádět pro platební karty Maestro.

FASTPAY

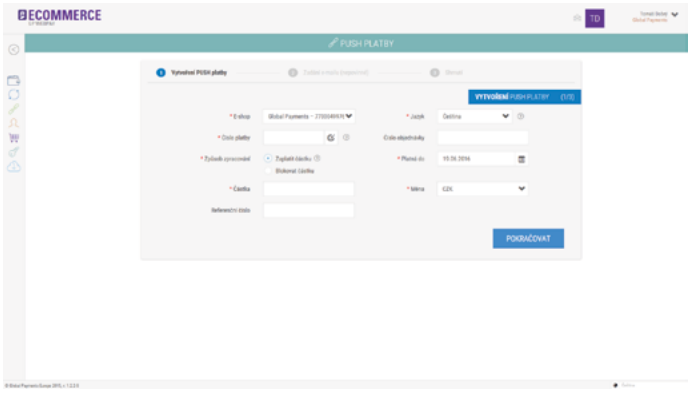
Funkce Fastpay umožňuje obchodníkovi zobrazit přihlášenému zákazníkovi na platební stránce poslední 4 číslice a platnost karty, kterou zákazník zaplatil předchozí platbu. Zákazník pouze zadá ověřovací kód (CVC2/CVV2), platba probíhá jako standardní platba 3D Secure s ověřením držitele platební karty.

Obchodník by měl zákazníka předem upozornit na využití této funkce.

Zákazník může zobrazené údaje přepsat a zaplatit jinou kartou.

PUSH platba – přijímání internetových objednávek

Funkce PUSH platba umožňuje obchodníkovi vytvořit požadavek na zaplacení (tzv. platební link). Obchodník může vytvořit PUSH platbu v portálu GP Webpay tak, jak je znázorněno na obrázku níže.



Platební link může být následně zákazníkovi zaslán emailem nebo může být převeden do QR kódu. Pokud se zákazník rozhodne PUSH platbu zaplatit, klikne na platební link, případně načte QR kód a jeho prohlížeč bude přesměrován na platební bránu GP Webpay, kde zaplatí platbu stejným způsobem jako v eshopu.

PORTÁL GP WEBPAY

Portál GP webpay uživateli obchodníka umožňuje:

- vyhledávání a správu plateb
- vytváření, zasílání, vyhledávání a správu PUSH plateb
- vytváření a správu uživatelů
- zobrazení statistiky a povolených funkcí pro eshop a platby
- vytváření a správu klíčů
- stažení technické dokumentace a dalších zdrojů pro integraci s rozhraním platební brány GP webpay

Kompletní informace o možnostech využití služeb GP Webpay naleznete v uživatelských příručkách dostupných online na adrese www.gpwebpay.cz

SPECIÁLNÍ TYPY TRANSAKCÍ

Tato sekce Vám představí řadu speciálních typů transakcí, které můžete potřebovat v závislosti na způsobu, jakým nabízíte zpracování transakcí prováděných kartou.

DCC – DYNAMIC CURRENCY CONVERSION

Služba DCC je již k dispozici prostřednictvím Vašeho platebního terminálu, vyžaduje však uzavření další dohody o službách. DCC služby jsou dostupné pro transakce s kartami Visa a Mastercard.

Nová příležitost pro Vaše podnikání

Služba DCC nabízí novou příležitost, jak vyhovět zahraničním držitelům karet, kteří dávají přednost nakupování ve své domácí měně. Ať už jsou na prázdninách či cestují za obchodem, mohou dostat možnost zaplatit v jejich domácí měně.

– Vaši zákazníci budou vědět přesně, kolik utratili ve své domácí měně, aniž by museli provádět jakýkoliv převod měny.

S touto službou nejsou spojeny žádné náklady za zřízení či jiné pravidelné poplatky. Poskytneme Vám vše, co potřebujete, abyste mohli svým zákazníkům nabídnout tuto skvělou možnost. Celkový proces platby je jasný a jednoduchý jak pro obchodníka, tak pro držitele karty.

– Systém DCC je plně automatický a POS software udělá práci za Vás.

Po skončení transakce dostane držitel karty účtenku, na níž se ukáže hodnota prodejní transakce v místní měně, směnný kurz a konečná částka účtovaná v měně země, která vydala kartu.

Navíc pokaždé, když zákazník dokončí nákup ve své domácí měně, obdržíte část výnosu z DCC a uvidíte to na svém Výpisu obchodníka. To povede ke snížení Vašich provozních nákladů a nárůstu zisků.

Výhody pro Vás

- DCC vytváří nový, trvalý zdroj kontinuálních výnosů
- Přináší Vám konkurenční výhodu na trhu
- Žádné poplatky za úvodní nastavení ani opakované poplatky
- Pomáhá růstu Vašeho podnikání tím, že přivádí zahraniční zákazníky

Výhody pro Vaše zákazníky

- Vědí, jaká přesná částka bude účtována v domácí měně zákazníka
- Snadné užití – vše dělá POS software, přičemž zůstává zachována známá nákupní zkušenost
- Osoby, které často jezdí na služební cesty, mohou těžit ze snadnějšího procesu hrazení výdajů
- Aktuální směnné kurzy
- Částka uvedená v moment prodeje je toutéž částkou, která bude klientovy účtována za jeho nákup
- S DCC se nepojí žádné skryté poplatky

Váš terminál na prodejním místě je připraven na použití DCC a provede automatickou detekci, zda je karta vhodná pro DCC. Poté můžete držiteli karty nabídnout možnost zaplatit v jeho domácí měně nebo v českých korunách. Pamatujte, že Váš zákazník musí dostat možnost učinit jednoznačnou volbu, zda chce transakci provést v domácí měně či v jakékoliv jiné navržené měně.

Částka je z účtu držitele karty odepsána v jeho lokální měně, držitel nebude tedy zatížen dalšími poplatky za konverzi měn u své vydavatelské banky. Na Váš bankovní účet bude přičtena částka v českých korunách, abyste nemuseli držet účty v cizích měnách.

DCC je podporováno v následujících měnách

EUR, PLN, RUB, DKK, NOK, CAD, USD, GBP, RON, SEK, HUF, CHF

Svému zákazníkovi poskytněte všechny dostupné možnosti a transparentnost

Podle směrnic společností Visa a Mastercard musí být každý držitel karty, který má možnost využívat službu DCC, informován o tom, že DCC je volitelná služba a že má možnost platit v českých korunách, pokud si to přeje. Koruny zůstávají výchozí měnou pro jakoukoliv transakci. Pokud POS identifikuje kartu jako způsobilou k využití

služby DCC, držitel karty dostane možnost vybrat si, v jaké měně chce zaplatit. Před tím, než proběhne autorizace, bude se zákazníkem potvrzena jeho domácí měna. Veškeré informace relevantní pro službu DCC budou držiteli karty k dispozici před dokončením transakce. Držitel karty bude mít k těmto informacím přístup prostřednictvím obrazovky na prodejním místě a tyto informace budou rovněž vytištěny poté, co bude dokončena DCC transakce.

Směnné kurzy

Směnné kurzy jsou dodávány a nastavovány na denní bázi společností Global Payments Europe. Jsou aplikovány na DCC transakce na Vašem prodejním místě.
Směnný kurz aplikovaný na DCC transakce je sdělen držiteli karty prodejním místem před dokončením transakce. Následně je jasně vytištěn na všech účtenkách k DCC transakci.

Vrácení peněz

Pro zpracování procesu vrácení peněz u DCC transakce budete muset zadat částku v českých korunách a následně po vyzvání zvolit možnost DCC. Zkontrolujte účtenku k původní transakci, abyste se ujistili, že byla zpracována jako DCC.
Kvůli rozdílům ve směnných kurzech může být konečná částka vrácená držiteli karty odlišná od hodnoty původní transakce v jeho domácí měně. Budete muset o této skutečnosti informovat držitele karty současně s tím, jak zpracováváte proces vrácení peněz.

Chargebacky

Pokud je DCC transakce vrácena zpět na kartu zákazníka z důvodu reklamace, bude částka transakce převedena z domácí měny držitele karty na české koruny buď společností Visa, nebo společností Mastercard předtím, než ji strhneme z Vašeho bankovního účtu. Kvůli rozdílům ve směnných kurzech je pravděpodobné, že konečná částka chargebacku se bude lišit od hodnoty původní transakce v českých korunách.
Budeme Vás písemně informovat o podrobnostech týkajících se jakéhokoliv procesu chargebacku, který je uplatněn vůči Vašemu bankovnímu účtu.

Předautorizace

Procedura DCC může být uplatněna rovněž při předautorizaci transakcí, když držitel karty provádí registraci (například v hotelu nebo v autopůjčovně). Současný směnný kurz uplatněný v DCC a částka v DCC měně musí být zobrazeny držiteli karty.
Je třeba držiteli karty jasně vysvětlit, že konečný DCC směnný kurz a DCC částka v jeho domácí měně bude určena až v momentě, kdy bude transakce zpracována při odhlášení z daného zařízení (hotelu atd.). Je možné, že držitelé karty si užití DCC při odhlášení rozmyslí. Pokud k tomu dojde, budou požádáni, aby navštívili recepci (příslušného hotelu či autopůjčovny).

Kontaktujte nás prosím s žádostí o další informace, pokud máte zájem nabízet svým zákazníkům službu DCC (kontaktní údaje jsou uvedeny na str. 54).

EET – ELEKTRONICKÁ EVIDENCE TRŽEB

- jde o elegantní a jednoduché řešení elektronické evidence veškerých transakcí na samostatném terminálu bez nutnosti integrace s pokladním systémem

- poskytuje přehled o každé transakci, ať už jste kdekoliv; jde o spolehlivý produkt, za nějž se můžeme zaručit

- na míru vytvořená řešení pro všechny oblasti podnikání
  – Platební terminál – jednoduché a snadné řešení pro malé podniky
  – Platební terminál napojený na stávající pokladní systém

Funkce a výhody

- jednoduchá aktivace služby

- registrace hotovosti, stravenek, platebních karet a dalších platebních metod

- možnost tisku účtenek

- přijímání platebních a stravenkových karet

- garantujeme dostupnost služby

EET Portál pro obchodníky

- přehled o všech transakcích na Vašem PC, mobilním telefonu nebo tabletu
- možnost registrace manuálně zadaných transakcí
- monitoring terminálu
- správa potvrzení pro komunikaci s finančním úřadem

Nastavení v portálu

Konfigurace pro každý jednotlivý terminál se nastaví primárně v EET portálu. Po přihlášení do portálu lze provést jednoduchou konfiguraci, podle které se automaticky nastaví a změní chování terminálu. Nejprve je třeba si zvolit, zda jste či nejste plátcem DPH. V případě že ano, je potřeba vybrat sazby DPH, ve kterých zboží nebo služby nabízíte. Dále je potřeba vybrat, zda prodáváte použité zboží, vouchery nebo cestovní služby.

Upozornění: Pokud například prodáváte použité zboží, je potřeba zadat jednotlivé sazby DPH pro nové a použité zboží zvlášť

Portál rovněž umožňuje nastavit pořadí v jakém je obsluha vyzvána terminálem k zadání částky v jednotlivých sazbách DPH, a to pro každý jednotlivý terminál. Rovněž je možné nastavit i pořadí preferovaných platebních metod tak, jak se budou zobrazovat na obrazovce Vašeho terminálu.

Každá úspěšná transakce je po zadání potřebných informací a po jejím úspěšném zakončení automaticky zaevidována na serveru finanční správy.

MULTICURRENCY – TRANSAKCE V CIZÍCH MĚNÁCH

Před zahájením přijímání plateb kartou, které zákazníkům umožňují provádět transakce v několika měnách, budete potřebovat náš předchozí písemný souhlas. K provádění prodejních transakcí a vracení peněz v cizí měně můžete přijímat karty Mastercard Credit, Visa Credit, Debit Mastercard, Visa Debit, Visa Electron, V PAY a Maestro.

Můžeme pro Vás zařídit, že budete moci přijímat platby ve vybraných cizích měnách, jako jsou eura, libry a americké dolary. Můžete si zvolit možnost, že veškeré Vaše transakce v cizích měnách budou přičítány přímo na vyhrazený účet v cizí měně. Připsané částky budou sdružovány podle měny, takže Vám bude za všechny transakce v dané měně připsána jedna částka a je třeba, abyste měli zvláštní bankovní účet pro každou přijímanou měnu. V opačném případě Vám bude příslušná transakce v cizí měně připsána na účet vedený v českých korunách.

Pokud byste se rádi dozvěděli více o přijímání transakcí v cizích měnách, kontaktujte nás prosím na čísle uvedeném na str. 54.

PROPOJENÍ TERMINÁLU S POKLADNÍM SYSTÉMEM (ECR)

Terminály, které nabízíme, umožňují propojení s pokladním systémem. Komunikační protokol mezi oběma zařízeními umožňuje vzdáleně ovládat funkce terminálu a řídit platební proces přímo z připojeného zařízení. K terminálu je možné se připojit přes rozhraní RS232, USB nebo přes TCP/IP. Po celou dobu implementace komunikačního protokolu jsme připraveni poskytnout Vám plnou technickou podporu včetně případného zapůjčení testovacího terminálu.

Pro více informací nás neváhejte prosím kontaktovat svého obchodního zástupce, který Vám rád poskytne bližší informace.

SPROPITNÉ

Spropitné je dodatečná částka přidaná k transakci držitelem karty, například když držitel karty platí účet v restauraci.

Další informace naleznete v Uživatelské příručce Vašeho terminálu.

CASHBACK

Služba CASHBACK umožňuje držiteli karty získat hotovost současně s nákupem zboží nebo služeb. Držitel karty zaplatí vyšší částku než je cena zboží/služby a přebývající částku dostane v hotovosti od obchodníka. Tato služba je poskytována držitelům karet, kteří mají vydané karty od banky působícím na českém trhu a má pro tuto službu certifikaci.

Tato služba je dostupná pouze u karet Visa, Visa Electron,

Mastercard a Maestro. Podmínkou možnosti využití služby CASHBACK je minimální nákup zboží či služeb v hodnotě 300,– CZK. Výběr hotovosti je umožněn do maximální výše 1500,– CZK. Celková částka musí být dělitelná na celé stokoruny.

Pokyny jak uskutečnit transakci tohoto typu naleznete v Uživatelské příručce pro Váš platební terminál.

AKCEPTACE STRAVENKOVÝCH KARET

Naše společnost nabízí možnost akceptace všech vydávaných stravenkových karet na platebních terminálech dodávaných naší společností.

Pro více informací neváhejte kontaktovat Vašeho obchodního zástupce.

SPECIFIKA AKCEPTACE PLATEBNÍCH KARET VE VYBRANÝCH ODVĚTVÍCH[3]

TRANSAKCE V HOTELECH A AUTOPŮJČOVNÁCH

Provozovatelé sítí platebních karet mají pro tyto transakce specifická pravidla. Tato sekce uvádí informace o procedurách, které musíte následovat při přijímání těchto transakcí. Váš terminál musí být nakonfigurován pro transakce předautorizace., Pokud si přejete aktivovat tuto možnost, kontaktujte nás (kontaktní údaje jsou uvedeny na str. 54). Detailní postupy jak provádět předautorizaci jsou popsány v Uživatelské příručce pro Váš platební terminál.

Pro účely této sekce jsou hosté a osoby, které si pronajímají automobil, považováni za držitele karty.

Základní kroky a postupy, které musí být při akceptaci karet dodrženy

- Všechny doklady poskytnuté zahraničnímu držiteli karty musí být dvojjazyčně (ČJ/AJ).
- Obchodník musí zajistit při rezervaci nebo stornování (včetně rezervací či storen přes internet) souhlas držitele platební karty s podmínkami rezervace.
- Obchodník má povinnost si veškerou korespondenci s držitelem karty uchovat pro případné pozdější doložení bance k řešení sporné transakce (reklamace).

Rezervace

Při rezervaci informujte držitele karty:

– o ceně ubytování či ceně za půjčení vozidla a sdělte mu číslo rezervace

– o detailech rezervace

– o obchodních podmínkách

– o podmínkách storna a eventuálně o čísle zrušení rezervace

[3] Tato sekce se vztahuje také na obchodníky, kteří mají na základě zvláštního povolení od naší společnosti možnost provádět příslušné typy transakcí (např. předautorizace).

Při přijímání rezervací pro hotely a autopůjčovny se ujistěte, že jste získali:

– jméno držitele karty

– adresu a telefonní číslo

– číslo jeho platební karty, datum začátku platnosti karty (pokud je dostupné) a datum ukončení platnosti

– souhlas s použitím platební karty

– souhlas s obchodními podmínkami

– souhlas s celkovou cenou, která bude účtována v den vytvoření rezervace

Pokud přijímáte rezervaci pokoje prostřednictvím karty Mastercard nebo Visa, musíte zaručit, že poskytnete alternativní ubytování stejného nebo lepšího standardu, za něž si nebudete účtovat žádný další poplatek, pokud se rezervované ubytování stane nedostupným.

Garantovaná rezervace

Garantovaná rezervace, je rezervace bez okamžitého inkasa částky ze strany obchodníka. Obchodník zajistí pro držitele karty rezervací a drží mu ubytování do plánovaného dne příjezdu. Držiteli karty musí být poskytnuta lhůta 24 hodin od doručení potvrzení rezervace na bezplatné zrušení rezervaci. Transakce je uskutečněna až za přítomnosti držitele karty.

Rezervace ubytování s Advance Deposit

Pokud hotel poskytuje rezervaci s možností Advance Deposit (nevratná záloha), musí být tato možnost uvedena v podmínkách rezervace, se kterými musí dát Držitel karty svůj souhlas.
Obchodník je povinen na účtence z terminálu uvést místo podpisu držitele karty „Advance Deposit“.

Registrace (check-in)

- Při příjezdu požádejte držitele karty o podpis registračního formuláře, který uvádí, že Vás držitel karty opravňuje odepsat peníze z jeho karty. Zkontrolujte, zda podpis odpovídá podpisu na kartě.

- Měla by být provedena předautorizace

- Informujte držitele karty o finančních prostředcích, které jste předautorizovali, a vyložte mu, jak jste k této částce došli (například započtením délky pobytu / vypůjčení, cenou pokoje/cenou za vypůjčení, příslušných daní, servisních poplatků a poplatků za kilometry).

Odhlášení (check-out)

- Pomocí kláves na terminálu zvolte Menu – Transakce – Předaut.zakonč., protáhnětě či vložte kartu, zadejte původní předautorizovanou částku, autorizační kód a identifikátor z účtenky předautorizace a postupujte podle pokynů na Vašem platebním terminálu.
  Je možné, že budete muset provést dodatečnou autorizaci, pokud je konečná částka:
  – nad Vaším autorizačním limitem
  – nad součtem dříve předautorizovaných částek (u karet Visa je povolená tolerance plus 15%, u Mastercard žádná tolerance povolená není). Autorizaci získejte pouze na rozdíl mezi předautorizovanou částkou či částkami a konečnou částkou.

- Kde je to možné, snažte se, aby byl konečný účet uhrazen za přítomnosti držitele karty a transakci proveďte s využitím ověření přes PIN.

- Nezapomeňte zrušit veškeré nevyužité autorizační kódy, pokud jste předautorizovanou částku přesáhli o více než 15% v případě transakce s kartou Visa.

- Nejste oprávněni uchovávat bezpečnostní kód karty (CSC). Pokud jste tuto informaci uchovali a pokud bude tato skutečnost později odhalena, může Vám být provozovatelem sítě platebních karet udělena pokuta.

- Společnost Mastercard vyžaduje, aby byla autorizovaná částka stejná, jako konečná hodnota odeslaná ke zpracování.

Zrušení rezervace

Držitel karty musí být seznámen s podmínkami pro zrušení rezervace již v okamžiku vytváření rezervace. Obecně musí platit tato pravidla:

– Garantované rezervace jsou drženy do následujícího dne po dni plánovaného příjezdu.

– Lhůta pro zrušení rezervace je 18.00 hod. (místního času) v den plánovaného příjezdu.

– Pokud uplatňujete dřívější lhůtu než 18.00 hod. (místního času) v den plánovaného příjezdu, sdělte tuto skutečnost držiteli karty.

– Den, čas lhůty a pravidla pro zrušení rezervace sdělte držiteli karty písemně.

– Obchodník nesmí požadovat podmínku bezplatného zrušení lhůty delší než 72 hodin před příjezdem hosta. Při stanovení delší lhůty než 72 hodin před příjezdem se reklamace držitele karty považuje za oprávněnou.

– Pokud není rezervace využita, nebo zrušena včas, držiteli karty se naúčtuje cena za první noc (vč. DPH), tzn. NO SHOW.

– Obchodník musí poskytnout držiteli karty kód zrušené rezervace.

NO SHOW

Transakce typu NO SHOW slouží pro dodatečné doúčtování služby, např. držitel karty si objedná službu (rezervace pokoje v hotelu / objednávka zapůjčení vozidla v autopůjčovně) a nezruší ji, nebo ji nezruší včas. Pokud dojde k tomuto případu, obchodník je oprávněn podle pravidel karetních asociací naúčtovat si jako odškodné jednu noc/jeden den.
Podmínky:

- Obchodník musí písemně informovat držitele karty o zatížení faxem nebo emailem.

- Obchodník musí mít informace o kartě (číslo karty, platnost karty).

- Obchodník musí mít písemnou objednávku na zboží nebo služby.

- Obchodník musí mít právo na doúčtování zapsáno ve svých podmínkách pro poskytování služeb.

- Obchodník s pomocí funkce „Prodej“ provede transakci na platebním terminálu a do místa určeného pro podpis vepíše čitelně hůlkovým písmem „NO SHOW“ (resp. „N.S.“).

Další poplatky

Hotely **nejsou** oprávněny postupovat ke zpracování transakce spojené s „dalšími poplatky“ za ztrátu, krádež či poškození hotelového vybavení bez souhlasu držitele karty. Tyto dodatečné poplatky nejsou garantované a mohou být odepsány z Vašeho účtu v případě, že držitel karty takovou transakci úspěšně reklamuje, čímž Vašemu podniku vznikne finanční ztráta.

Autopůjčovny: Pouze společnost Visa povoluje zákazníkovi účtovat zpětné či pozměněné částky v důsledku poškození půjčeného vozidla, za palivo, pojištění, parkování, pokuty, poplatky za půjčení a daně. Musíte však být schopni dodat **vše** níže uvedené:

- kopii smlouvy o půjčení
- odhad výše škod od organizace, která je oprávněna provádět opravy v zemi, kde sídlí autopůjčovna
- případnou policejní zprávu o nehodě
- dokumentaci obsahující souhlas držitele karty, že škody uhradí svou Visa kartou
- jakoukoliv jinou dostupnou relevantní dokumentaci, která prokazuje odpovědnost držitele karty za vzniklou škodu
- kopii pojistky automobilu v případě, že po držiteli karty vyžadujete, aby zaplatil pojištění, jehož výše bude odečtena od výše hrazených škod. Místo pojistky Vaší autopůjčovny můžete poskytnout kopii smlouvy o půjčení vozidla, která potvrzuje souhlas držitele karty, že bude hradit podíl na krytí pojistné události. V tomto případě je nutné, aby držitel karty předtím podepsal či připojil své iniciály k části smlouvy, která uvádí informace o pojištění.

Společnosti Mastercard a Maestro nedovolují, aby autopůjčovny účtovaly zákazníkům zpětné nebo pozměněné částky. Jakékoliv poplatky za ztráty či odcizení musí být zpracovány zvlášť a musíte pro toto zpracování získat souhlas držitele karty.

SMĚNÁRNY/CASINA

Abyste mohli přijímat platby kartou za služby směnárny nebo casina, potřebujete náš předchozí písemný souhlas.

Musíte provést důkladně veškeré kontroly karet, tak jak jsou popsány v kapitole Kontrola karet (viz strana 13).

Vedle těchto kontrol jste při provádění transakcí v rámci směnárny povinni identifikovat držitele karty a provést záznam o předloženém průkazu totožnosti. Přesné požadavky závisí na typu použité karty a mějte prosím na paměti, že i zde hrozí riziko chargebacků.

Na obchodním místě typu Směnárna/Casino není povoleno provádět transakci Návrat.

PŘIPISOVÁNÍ A ODEPISOVÁNÍ PLATEB Z VAŠEHO BANKOVNÍHO ÚČTU

PŘIPISOVÁNÍ PLATEB NA VÁŠ BANKOVNÍ ÚČET

Zpracování a zúčtování transakcí

Naše společnost poskytuje automatické zúčtování transakcí, které je zcela nezávislé na prováděných uzávěrkách. V základním nastavení každý terminál provádí automatickou uzávěrku[4], a to v tzv. hodinovém oknu pro provedení uzávěrky (- 30 minut až + 30 minut od času uzávěrky). Hodinové okno pro uzávěrku může být z různých důvodů zúčtovacích procesů nastaveno kdykoliv mezi 0:00 – 22:55.

Existují následující typy uzávěrek, které je možné provést:

- Předčasná uzávěrka - Pokud je provedena uzávěrka před oknem pro uzávěrku (ručně), nemá tato uzávěrka na zpracování transakcí žádný vliv a slouží pouze pro Vaše vnitřní potřeby. Veškeré následující transakce se až do provedení automatické uzávěrky nadále zahrnují do zúčtování za tento den a budou Vám proplaceny v jedné částce.

- Řádná uzávěrka - Pokud je provedena uzávěrka v rámci přiřazeného okna (ruční nebo automatická), uzavře se účtování pro daný den a následující transakce se účtují do následujícího dne.

- Zpožděná uzávěrka – Pokud je uzávěrka provedena po čase určeném pro okno pro uzávěrku (ručně), budou veškeré transakce uskutečněné do konce okna pro uzávěrku zúčtovány v daný den. Transakce provedené od konce okna pro uzávěrku až do okamžiku provedení ruční zpožděné uzávěrky budou zúčtovány v následujícím dni.

Lhůty pro zpracování

Po obdržení dokladu o Vaší transakci tuto transakci postoupíme na příslušného vydavatele karty, od nějž budeme za Vás vyžadovat platbu (viz „Zpracování transakcí na str. 24), a to ve stejný den, kdy nám tyto transakce předložíte. V případě, že transakce předložíte po systémové lhůtě pro odeslání transakcí ke zpracování (která je v 22:55), anebo v den, který není pracovním dnem, postoupíme tyto transakce vydavateli karty až v následující pracovní den.

Lhůty pro připsání platby na Váš účet

Platba bude provedena na Váš bankovní účet či jiným způsobem stanoveným ve Všeobecných obchodních podmínkách pro akceptaci platebních karet. Obvykle odesíláme finanční prostředky následující den poté, co úspěšně obdržíme Vaší transakci zpracovanou elektronicky pomocí Vašeho platebního terminálu. Datum, kdy bude částka připsána na Vašem účtu, závisí na bance, u níž je Váš účet veden.

PORTÁL PRO OBCHODNÍKY (MERCHANT PORTAL)

Klientský portál je systém určený všem obchodníkům akceptujícím platební karty prostřednictvím Global Payments. Poskytne Vám přehled vašich plateb, transakcí, blokací a umožní Vám získat výpisy ve formátu PDF, XLSX a také různé jiné reporty. Tyto funkce Vám mohou být užitečné při rekonciliaci vašich plateb a kontrole transakcí, které byly odeslány ke zpracování do Global Payments z vašich terminálů.

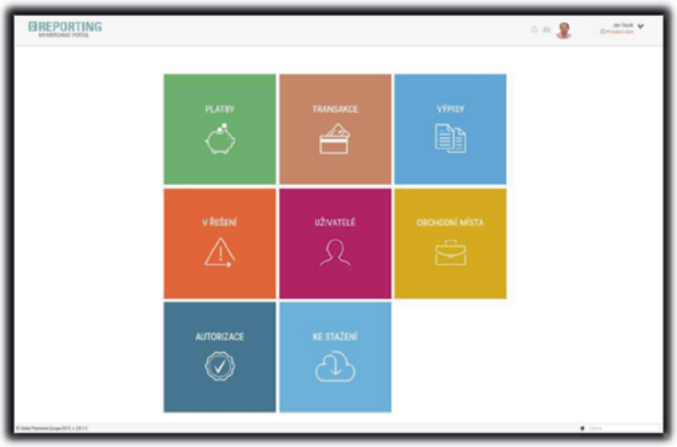
Portál Vám zároveň umožňuje přístup k časově důležitým a finančně citlivým informacím a dává Vám flexibilitu, kterou papírové výpisy neumožňují. Všechna data jsou doplňována na denní bázi a jednotlivé transakce jsou zobrazovány se všemi souvisejícími detaily.

V průběhu kontroly vašich plateb a transakcí můžete dělat následující:

- Zobrazit platby mezi dvěma časovými okamžiky
- Zobrazit sumáře pro vybrané platby
- Zobrazit jednotlivé transakce, které vytváří danou platbu
- Ověřit stvrzenky vašich transakcí
- Vyhledávat konkrétní finanční data
- Třídit data podle jednotlivých plateb, data transakce, platby, obchodního místa, částky, terminálu
- Zobrazit data pro jedno nebo více vašich obchodních míst

[4] Na základě požadavku lze změnit na ruční uzávěrku

• Analyzovat data – exportovat a stáhnout výběr dat do vašeho PC ve formátu XLS a použít běžné aplikace určené k analýze dat.



Dostupnost a historie dat

Data v portálu jsou dostupná 24 - 48 hodin po uzavírce terminálu. Samotný portál je dostupný nonstop, 24 hodin denně, 7 dní v týdnu. K dispozici je 2 letá platební historie.

Podrobnější informace s přesným popisem všech dostupných funkčností naleznete v Uživatelské příručce pro Klientský portál.

VÝPISY

Výpisy jsou k dispozici ke stažení v sekci „Výpisy" v Merchant Portálu. Ke stažení jsou k dispozici následující dokumenty: výpisy plateb, faktury a opravy faktur za pronájem terminálů, storna faktur, upomínky a různé další reporty.

Výpisy nejsou automaticky zasílány na Vaši emailovou adresu.

Formáty výpisů

• *.pdf: uživatelsky přívětivé shrnutí uzavřených transakcí, které je vhodné k manuálnímu zpracování – načtení do účetního systému není možné

•.flat, *.xml: vhodné pro elektronické zpracování, odeslání emailem, SFTP nebo na portál obchodníka. Je vyžadována instalace vhodného účetního software. Pro manuální zpracovávání tohoto formátu jej lze otevřít v programu MS Excel

• Merchant portal – internetová aplikace, která umožňuje prohlížet platby, transakce a autorizace, umožňuje vygenerování souboru ve formátu .pdf nebo .xlsx

Typy výpisů

Detailní – obsahuje základní informace a úplné shrnutí všech transakcí zpracovaných za definované časové období. Doporučený typ.

Četnost výpisů
•.pdf formát
– Denně
– Týdně
– Měsíčně

•.xml.flat formát
– Denně

ZAMÍTNUTÉ TRANSAKCE

V rámci námi prováděného procesu ověřování transakcí zamítneme a vrátíme veškeré transakce, které neprošly ověřením, například transakce provedené prošlou kartou. Zamítnuté transakce Vám způsobí finanční ztrátu.

Než k tomu dojde, prověříme detaily transakce a naše systémy. Pokud nalezneme jakékoliv chyby, budou opraveny. Pokud nedojde k vyřešení problému, budeme Vás informovat dopisem/emailem a částka připsaná na Váš účet bude příslušným způsobem upravena.

Pokud dojde k zamítnutí celého souboru s transakcemi, budeme Vás telefonicky kontaktovat a budeme Vás informovat o nápravných opatřeních, abyste se vyhnuli situaci, že na Váš účet nebudou připsány žádné finanční prostředky.

SERVISNÍ POPLATKY

Jde o částku, kterou jste povinni uhradit za námi poskytované služby zpracování transakcí prováděných platební kartou. Poplatky jsou nejčastěji vypočteny jako procento z částky transakce.

Detailní informace o servisních poplatcích naleznete ve Vaší Žádosti o akceptaci platebních karet.

REKONCILIACE

Důrazně doporučujeme, abyste prováděli rekonciliaci svého bankovního účtu každý měsíc. Prosím zavolejte nám nebo pošlete email (kontaktní informace jsou uvedeny na str. 54), pokud máte jakékoliv dotazy ohledně položek na výpisech týkajících se zpracování transakcí platební kartou.

CHARGEBACKY

ÚVOD

Chargebackem se rozumí transakce, kterou si vydavatelská banka bere zpět celou, nebo částečnou hodnotu transakce proplacené obchodníkovi a to zpravidla na základě reklamace podané držitelem platební karty. Chargeback je někdy též nazýván jako „spor" (dispute).

Každý chargeback má specifická pravidla a vztahují se na něj specifická nařízení a časové lhůty, v jejichž rámci musí Global Payments jednat. Tato pravidla nastavují společnosti Mastercard, Visa, JCB a UnionPay International a určují, jaké kroky můžeme podniknout, pokud řešíme případ chargebacku. Uděláme vše, co je v rámci těchto pravidel možné, abychom před chargebackem ochránili.

Existuje řada různých důvodů, proč může být transakce reklamována a následně její částka odepsána z účtu obchodníka; tyto důvody nicméně spadají do pěti hlavních kategorií:

- žádost o dokumentci (viz „Co je žádost o dokumentaci?" níže)
- neoprávněná transakce – oprávněný držitel karty nedal k takové transakci souhlas a nepodílel se na ní
- důvody související s autorizací – například, že transakce přesahuje autorizační limit a byla dokončena bez autorizace (viz strana 22), autorizace byla zamítnuta atd.
- chyba při zpracování – například duplicitní zpracování transakce
- zrušené/vrácené zboží nebo služby – držitel karty zrušil objednávky nebo vrátil zboží a nebyly mu vráceny peníze, vrácení peněz nebylo zpracováno anebo vrácené peníze nebyly připsány na stejnou kartu, z jaké byly původně odepsány (viz strana 24)
- nedoručené zboží/služby – například v případě pozdního dodání zboží nebo služeb nebo v případě dodání nesprávného zboží.

O chargebacku Vás vždy budeme informovat dopisem nebo emailem před tím, než budou z Vašeho účtu odepsány finanční prostředky. Zda Vás budeme schopni před chargebackem ochránit, závisí na tom, jestli byla daná transakce plně v souladu s pravidly stanovenými společnostmi Mastercard, Visa, JCB, nebo China UnionPay. Kde je to možné, například tam, kde byla transakce autentizována načtením čipu a zadáním PIN, budeme Vás proti chargebacku automaticky bránit. V případě, že od Vás budeme vyžadovat další informace/dokumentaci obdržíte od nás písemnou výzvu. Chargeback (sporná částka) Vám bude účtován až po ukončení celého chargebackového procesu.

Pokud Vás písemně kontaktujeme s žádostí o informace, je velmi důležité, abyste požadované informace dodali, a to v jasné podobě a ve lhůtě stanovené v našem dopise. Pokud tak neučiníte, může nám to zabránit v jakékoliv další Vaší obraně před chargebackem v rámci daných časových možností.

Požadavky na dodání této dokumentace lze vznášet až do 540 dní poté, co byla transakce odepsána z účtu držitele karty či co byla obdržena daná služba. Nicméně v některých případech, například tam, kde šlo o podvod, mohou být dokumenty vyžádány až do dvou let po datu transakce. Je proto klíčové, abyste mohli tuto dokumentaci snadno poskytnout. Pamatujte, že údaje z karet musí být bezpečně uschovány (viz str. 44 o „Datové bezpečnosti")

Kontaktujte nás prosím (kontaktní údaje jsou uvedeny na str. 54), pokud s námi potřebujete prodiskutovat dopis oznamující chargeback či pokud si nejste jisti, jaká dokumentace je od Vás vyžadována.

CO JE ŽÁDOST O DOKUMENTACI?

Žádost o dokumentaci bývá podána v případech, kdy držitel karty vznese dotaz týkající se transakce provedené platební kartou. Často je to proto, že si držitel karty nemůže vzpomenout, že by transakci prováděl.
Žádost o dokumentaci není chargeback. To znamená, že Vám nebudeme z účtu strhávat žádné peníze. Žádost o dokumentaci však může v chargeback vyústit, pokud informace, které od nás vydavatel karty získá, je nečitelná, nepostačuje k tomu, aby byl zodpovězen dotaz držitele karty, nebo neprokáže autentizaci klienta prostřednictvím čipu na kartě ve spojení s ověřením PIN, nebo autentizaci prostřednictvím zabezpečené internetové platby.

Je důležité, abyste na žádost o dokumentaci okamžitě odpověděli, neboť pokud tak neučiníte, můžeme podle pravidel Mastercard, Visa, JCB a China UnionPay

ztratit právo na to, bránit Vás proti jakýmkoliv dalším chargebackům.

JAK SE VYHNOUT CHARGEBACKŮM

Transakce, kde je karta přítomna (CP)

Čipové karty a terminály se zadáváním PIN výrazně pokročily v prevenci podvodů s kartami a v současné době představují standard.

Standardy provozovatelů sítí platebních karet vyžadují, aby CP transakce, kde je předložena čipová karta s PIN, byly provedeny načtením čipu a zadáním PIN do terminálu. Použití magnetického proužku namísto čipu je povoleno, pokud Vás terminál po vložení čipu vyzve, abyste použili magnetický proužek.

V oběhu je stále řada platných karet, které neobsahují čip a je třeba je protáhnout čtečkou a přečíst data z magnetického proužku. Poté se může stát, že budete muset k ověření transakce použít podpis držitele karty. Rovněž existuje řada karet, které mají čip, ale vyžadují k ověření pouze podpis držitele karty. Řada těchto karet byla vydána v zahraničí nebo držitelům karet, kteří nejsou schopni použít PIN.

Nejlepším způsobem, jak minimalizovat riziko chargebacků u CP transakcí je pozorně následovat výzvy, které se objevují na Vašem terminálu. Pokud terminál autorizuje platbu a vyzve držitele karty k podpisu, pak by tato procedura měla být povolena s tím, že je třeba provést běžné kontroly pro transakce ověřované podpisem (viz strana 12).

Transakce, kdy je karta nepřítomna (CNP)

V prostředí CNP je důležité mít na paměti, že jste vystaveni vyššímu riziku chargebacků. Pokud budete následovat níže uvedené body a rovněž se řídit informacemi uvedenými v sekci „Jak snížit riziko podvodu“ na str. 48, bude toto riziko sníženo na minimální míru:

- Pokud zákazník žádá o vyzvednutí zboží v obchodě, proveďte transakci při vyzvednutí jako transakci, kdy je karta přítomna, a to pomocí Vašeho zařízení na obchodním místě.
- Zboží vždy odesílejte doporučenou nebo zvláštní poštou či prostřednictvím důvěryhodného a bezpečného dopravce. Trvejte na tom, že musí být vystaven doklad o doručení, který musí být následně podepsán, pokud možno držitelem karty. Požádejte kurýra, aby zásilku nedoručil, pokud se prostory, kam má být doručena, zdají prázdné. Mějte prosím na paměti, že doklad o zaplacení jako takový není dostatečným důkazem, který by Vás ochránil před chargebackem.
- Nikdy nepředávejte zboží třetím stranám, jako jsou například řidiči taxi nebo messengeři.
- Dbejte zvýšené opatrnosti u transakcí, kde je fakturační adresa odlišná od požadované doručovací adresy. Vyhněte se doručování na adresy, které jsou odlišné od adresy držitele karty, jako jsou například hotely, internetové kavárny a adresy jiných osob, u nichž se adresát zdržuje.
- Opatrně postupujte u požadavků na dodání do druhého dne, požadavků na rychlou změnu doručovací adresy, u telefonátů v den doručení, v nichž se kupující požaduje určitý čas doručení.
- Zvýšené pozornosti dbejte tehdy, když objednávka přišla z emailového účtu, v němž není zákazníkovo jméno nějakým způsobem obsaženo v emailové adrese.
- Buďte podezřívaví vůči transakcím, které jsou vzhledem k typu Vašeho podnikání nezvykle vysoké co do hodnoty a objemu, případně je prodej „příliš snadný“. Naše zkušenosti nám říkají, že právě u těchto transakcí je zvýšená pravděpodobnost, že budou podvodné.
- Pokud vracíte peníze, vždy je vraťte na stejnou platební kartu, s níž byla provedena původní transakce.
- Veďte si databázi reklamovaných transakcí (chargebacků), abyste mohli snáze odhalit vzorce v podvodných transakcích. Pokud se prodej zdá být „příliš dobrý na to, aby byl skutečný“, pak zřejmě skutečný není. Nebojte se kontaktovat držitele karty, abyste mu položili doplňující otázky či si vyžádali dodatečnou identifikaci. Poctivý zákazník by měl ocenit, že Vám záleží na bezpečnosti a že se snažíte své zákazníky ochránit před podvody.
- Pro transakce v rámci internetových obchodů by měla být na internetových stránkách implementována

ještě další úroveň zabezpečení. Funkce Mastercard SecureCode a Verified by Visa (VbV) byly vytvořeny, aby umožnily zákazníkům prokázat se jako skutečný držitel karty (viz str. 12). Abyste mohli přijímat karty Maestro přes internet, musíte podporovat Mastercard SecureCode.

Většina chargebacků vzniká jako následek podvodných transakcí. Pokud dokončíte transakci, která se jeví jako podvodná, činíte tak na své vlastní riziko. Pokud byla transakce dokončena, ale zboží nebylo odesláno, stále jste v pozici, kdy můžete zákazníkovi vrátit peníze.

Získání úspěšné autorizace

Autorizace transakce platební kartou je způsobem, jak si ověřit, že karta nebyla ztracena/odcizena a že držitel karty má v okamžiku provedení platby na svém účtu dostatečné finanční prostředky.

Úspěšná autorizace není ověřením identifikace Držitele karty a tudíž není ani garancí, že bude proplacena.

Doklad převzetí zboží

Vizte prosím kapitolu „Dodání zboží“ na str. 40 pro více informací o dodání zboží a důležitosti získat doklad o dodání. Mějte prosím na paměti, že samotný doklad o dodání není dostatečným důkazem, který by odvrátil chargeback.

Pokud dokončujete prodej zboží či služeb mimo Vaše obchodní prostory, doporučujeme k validaci transakce využít mobilní terminál. Pokud je transakce následně reklamována, budeme požadovat důkaz, že karta a držitel karty byli přítomni v čase transakce.

Přijetí zálohy – Zboží je objednáno, ale není ihned doručeno

Někdy se mluví také o „pozdrženém dodání“ a obvykle se používá u transakcí, kde není možné ihned dodat zakoupené zboží, například jde-li o velký kus nábytku, který byl vyroben na míru. V těchto případech můžete vyžadovat, aby držitel karty provedl nákup ve dvou oddělených transakcích, kdy první transakcí složí zálohu a druhou splatí zbývající částku.
Pokud je prodej proveden touto metodou, je důležité, aby obě transakce byly zpracovány odděleně a druhá přijatá transakce nebyla zpracována, dokud nebylo zboží odesláno. Pokud zpracujete přijatou transakci, jíž byla uhrazena zbývající částka, dříve, než bylo zboží odesláno, držitel karty to může vnímat jako „nedodání zboží“ a požadovat u vydavatele karty, aby mu byla vrácena částka transakce pomocí chargebacku.

Pravidla provozovatelů sítí platebních karet stanovují, že přijatá transakce, jíž byla uhrazena záloha, může být postoupena ke zpracování před tím, než došlo k odeslání zboží nebo služeb. Přijatá transakce, jíž byla uhrazena zbývající částka, však nesmí být postoupena ke zpracování, dokud nebylo zboží odesláno.

Nepřijetí zboží či neposkytnutí služeb

- Nezpracovávejte transakci platební kartou, dokud nedošlo k odeslání zboží či poskytnutí služeb.
- Nezpracovávejte žádné transakce platební kartou, kde již držitel karty zaplatil za zboží nebo služby pomocí jiného způsobu platby.
- Držitele karty nechte podepsat Váš doklad o doručení či doklad o poskytnutí služeb poté, co jste danou služby dokončili.
- Pokud nejste schopni doručit zboží a služby v plném rozsahu, neustále informujte držitele karty o všech Vašich krocích.
- Pokud jste držiteli karty účtovali za zboží, které ještě nemůže být odesláno, proveďte jen částečnou transakci. Získejte autorizaci na hodnotu zboží, které jste schopni odeslat.

Zboží neodpovídá popisu

- Je Vaší povinností zajistit, že zboží objednané držitelem karty je dodáno či poskytnuto přesně tak, jak je popsáno ve Vašem katalogu či v rámci Vaší reklamy. Pokud nejste schopni dodat přesnou specifikaci včetně barvy, velikosti, kvality a kvantity, pak musíte držitele karty upozornit na změnu a požádat jej o schválení pozměněné varianty.
- Zboží by mělo být doručeno včas a mělo by být vhodné

k účelu, za jakým bylo objednáno: za přijatelné například nelze považovat lístky do divadla, které dorazily po datu představení.

- Pokud držitel karty obdrží zboží, a to je poškozeno, rozbito či je jinak nevhodné k požadovanému účelu, pak bude mít držitel karty právo požadovat od Vás vrácení částky transakce (chargeback).

- V případě, že Vám držitel karty zboží vrátí, pak máte povinnost vrátit držiteli okamžitě plnou částku, kterou za zboží zaplatil.

Další důvody pro chargeback

Níže jsou uvedeny některé další běžné důvody pro chargeback. Nemá jít o vyčerpávající seznam a za předpokladu, že se budete řídit doporučeními uvedenými v těchto Pokynech pro obchodníky, měli byste být schopni se chargebackům vyhnout.

- transakce zpracovaná na prošlé kartě

- nesprávná částka transakce – držiteli karty bylo účtováno více, než skutečně převzal či než o čem byl informován

- nesprávná měna transakce – držiteli karty byla transakce zaúčtována v jiné měně, než jakou aktivně odsouhlasil

- klient nedal aktivní souhlas s doúčtováním dodatečné transakce

PCI DSS/BEZPEČNÁ AKCEPTACE PLATEBNÍCH KARET

V okamžiku, kdy přijímáte platební kartu k realizaci bezhotovostní transakce, je nezbytné vzít v potaz hodnotu dat, které v rámci platební transakce shromažďujete a s tím spojenou ochranu těchto dat.Pokud by došlo k bezpečnostnímu incidentu, vystavujete se riziku finančních ztrát a poškození pověsti Vašeho podnikání.

Standard Payment Card Industry Data Security Standard (PCI DSS) obsahuje mezinárodně závazná pravidla bezpečného zacházení s údaji o platební kartě a údaji z transakce, které byly zavedeny kartovými společnostmi s cílem zvýšit úroveň zabezpečení tohoto typu dat.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

PCI DSS je souborem 12 komplexních požadavků na zabezpečení zákaznických dat z platebních karet. Patří mezi ně požadavky na správu zabezpečení, směrnice, procedury, síťovou architekturu, podobu software a další klíčová ochranná opatření.

Cílem standardu je pomoci organizacím chránit zákaznická data z platebních karet v každodenním byznysu. Osobní, citlivá data uložená na kartě či v kartě představují klíč pro uskutečnění transakce. Pokud tato data náležitě neochráníte, může se stát, že podvodníci, kteří objeví zranitelná místa Vašeho systému a podaří se jim do systému nabourat, data odcizí. Tato data jsou pro ně velmi cenná, neboť je mohou zneužít k financování další nelegální činnosti.

Jde o velmi reálnou hrozbu. Každý obchodník, ať už je jeho podnik jakkoliv velký, je vystaven riziku úniku dat. Následkem může být pokuta udělená provozovatelem sítě platebních karet, protože zákaznická data nebyla zabezpečena dostatečně efektivně a podle PCI DSS standardů. Tyto pokuty začínají na částce 5000, ale v závislosti na konkrétních okolnostech mohou být mnohem vyšší.

Doporučené postupy

V principu soulad se standardem PCI DSS znamená, že nakládáte s finančními údaji z platebních karet, jako by šlo o hotovost. Měli byste zajistit, že s daty je nakládáno tak bezpečně, jak je to jen možné, a to minimálně tím, že:

- informace z platebních karet nebudete poskytovat nikomu jinému, pouze nám
- omezíte přístup Vašich zaměstnanců k datům z platebních karet.

Za žádných okolností neuchovávejte následující informace:

- plný rozsah údajů uložených na magnetickém proužku nebo v čipu – rovněž známých jako Track 2 Data –, například ověřovací hodnotu karty (Card Verification Value, CVV, Batch Code), validační kód karty (CVC) a verifikační hodnotu PIN (Pin Verification Value, PVV).
- Validační kód karty (CVC – musí být smazán, jakmile jste autorizovali transakci, dokonce i v případě CNP transakcí, jako jsou například objednávky poštou či telefonem (MOTO) či nezabezpečené internetové transakce.

Je velmi důležité, abyste zavedli následující procedury:

- uchovávejte jen ta citlivá data, která jsou nezbytná pro Vaše podnikání, po dobu nezbytně nutnou
- uchovávejte veškerý materiál obsahující informace o kartách (např. účtenky z transakcí) v uzamčeném, bezpečném prostoru, po dobu nezbytně nutnou
- zničte či smažte veškerá média obsahující zastaralá data z transakcí, která obsahují informace o držiteli karty, bez odkladu
- zajistěte, že všechny třetí strany, které pro Vás zpracovávají nebo ukládají citlivá data, nebo ty strany, se kterými o těchto službách jednáte, potvrdili, že splňují standard PCI DSS a jsou zaregistrovány na stránkách kartových společností (Visa, Mastercard)
- bezpečně uchovávejte účtenky z transakcí po dobu stanovenou místní legislativou, od dodání zboží či služeb a po uplynutí této doby zajistěte jejich bezpečné znehodnocení
- údaje o držitelích karet uchovávejte, jen je-li to nezbytně nutné; v každém případě však tyto údaje musí být uloženy bezpečně a musí být šifrovány

Ať už sami vytváříte, revidujete či navrhujete počítačové systémy či je nakupujete prostřednictvím třetí strany, která ukládá, zpracovává a přenáší citlivá data z platebních karet, je důležité, abyste zajistili, že se tento systém a příslušná třetí strana řídí standardem PCI DSS. Dodavatelé služeb a aplikací, kteří prošli auditem PCI DSS a PA-DSS, jsou uvedeni na oficiálních stránkách PCI DSS Rady **https://www.pcisecuritystandards.org/**.

Pokud na svém pokladním zařízení používáte volně prodejný software, máte povinnost, uloženou provozovateli sítí platebních karet, zajistit, že tento software splňuje standard Payment Application Data Security Standard (PA-DSS). Užívání software, který tomuto standardu neodpovídá, porušuje pravidla stanovená provozovateli sítí platebních karet a vystavujete se tím riziku výrazných postihů, dalších nákladů a pokut. Rovněž tím zvyšujete riziko, že dojde k úniku dat s významným finančním a reputačním dopadem na Vaše podnikání.

Veškeré námi dodávané vybavení pro akceptaci platebních karet je v souladu s aktuálně platnou verzí PCI DSS standardu. Díky tomu bude pro Váš podnik snazší dosáhnout souladu s PCI DSS.

Pro další informace o PCI DSS navštivte:

- **http://www.pcisecuritystandards.org** – tato stránka obsahuje nejnovější verzi standardů PCI DSS a doporučení, jak tyto standardy dodržovat
- http://www.mastercard.com/us/sdp/merchants/index.html
- http://www.visaeurope.com/receiving-payments/security

VAŠE POVINNOSTI

Dodržování Standardu PCI DSS

V rámci Smlouvy o zpracování transakcí platební kartou, kterou máte s námi uzavřenou, je od Vás vyžadováno, abyste dodržovali standard PCI DSS.

Všichni obchodníci budou spadat do jedné ze čtyř kategorií obchodníků na základě objemu transakcí za období posledních 12 měsíců. Následující tabulka udává objem transakcí pro každou úroveň a validační metodu, kterou musíte použít.

ÚROVEŇ	KRITÉRIA	VALIDAČNÍ PROCEDURY	PROVÁDĚNÉ
1	Přes 6 000 000 transakcí s kartami Mastercard a Visa za rok	• Výroční bezpečnostní audit v sídle společnosti a Report on Compliance (ROC) • Čtvrtletní skenování sítě	Kvalifikovaným bezpečnostním hodnotitelem (QSA, Qualified Security Advisor)
2	Mezi 1 000 000 a 6 000 000 transakcí s kartami Mastercard a Visa za rok	• Výroční bezpečnostní audit v sídle společnosti (včetně ROC) • Čtvrtletní skenování sítě	QSA nebo interní bezpečnostní hodnotitel (ISA, Internal Security Assessor)
3	Mezi 20 000 a 1 000 000 transakcí v internetovém obchodě za rok	• Výroční PCI sebehodnotící dotazník (SAQ, Self-Assessement Quesitonnaire) • Čtvrtletní skenování sítě	Sebehodnotící dotazník
4	Méně jak 20 000 transakcí v internetovém obchodě a méně než 1 000 000 transakcí za rok	• Výroční PCI SAQ • Čtvrtletní skenování sítě	Sebehodnotící dotazník

Úplný seznam kvalifikovaných QSA naleznete na stránkách PCI Security Standards Council:

https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

Následující stránka poskytuje informace o tom, jak se stát ISA:

https://www.pcisecuritystandards.org/approved_companies_providers/internal_security_assessors.php

Je třeba, abyste nám pravidelně dokládali, že dodržujete standardy PCI DSS. Proto nám prosím zašlete následující:

- Vaše písemné potvrzení o dodržování standardů:
- Attestation of Compliance (je součástí SAQ dokumentace) pro obchodníky, kteří si provádějí audit sami, ve spolupráci s ISA (ročně)
- Report on Compliance (ROC) u obchodníků, u kterých provedl audit externí auditor (ročně)
- ASV – doklad o výsledku skenu sítě (čtvrtletně)
- pokud využíváte třetí stranu, pak také kopii AOC této třetí strany

Zašlete prosím výše zmíněné dokumenty Vašemu obchodnímu zástupci nebo přímo PCI DSS teamu na adresu pci@globalpayments.cz nebo zavolejte na náš helpdesk (kontaktní údaje jsou uvedeny na str. 54), pokud potřebujete jakékoliv další informace.

TŘETÍ STRANY

Pokud využíváte služeb třetí strany a poskytnete této společnosti přístup k údajům karet a finančním údajům držitelů karet pro jakýkoliv účel (např. zpracování transakce, uložení dat nebo služby call centra), budete muset zajistit, že i tato třetí strana dodržuje veškerá pravidla a nařízení v oblasti datové bezpečnosti. Zvláště pak musí veškeré třetí strany, které za Vás ukládají či zpracovávají tato data, dodržovat standard PCI DSS a musí být registrovány u kartových společností. Za jakékoliv nesplnění těchto požadavků s Vámi spolupracující třetí stranou ponesete odpovědnost Vy a můžete se tím vystavit zbytečnému riziku finančních ztrát.

Je vyžadována kopie AOC třetích stran. Zašlete ji prosím na výše uvedenou adresu.

Oblast cestovního ruchu je velmi rizikovým segmentem z pohledu úniku dat platební karty a soukromých dat jejich držitelů, které vede nejenom k výrazným finančním ztrátám, ale i ke ztrátě reputace daného subjektu nebo řetězce. Subjekty segmentu cestovního ruchu musí doložit i AOC dodavatele Hotel Management Systemu a společností, které provádějí služby pro obchodníka, jako např. rezervace, placení záloh atp.

CO SE STANE, POKUD NEDOSÁHNETE SOULADU S PCI DSS?

Pokud neprokážete svůj soulad s tímto standardem, mohou na Vás být uvaleny měsíční poplatky za nedodržování požadavků na bezpečnost, které jsou účtovány zpětně a jsou nevratné. Tyto poplatky za nedodržování PCI DSS standardu budou pokračovat, dokud opět nedosáhnete souladu s PCI DSS.

Ať už si zvolíte jakoukoliv cestu, jak dosáhnout souladu, nebudete považováni za subjekt, který dodržuje standard PCI DSS, dokud jsme neobdrželi a nenahlásili Váš status v této oblasti u kartových společností.

POKUD MÁTE PODEZŘENÍ NA PORUŠENÍ BEZPEČNOSTI

Pokud se budete řídit výše doporučenými postupy a pokud dosáhnete plného souladu se standardem PCI DSS, pak se Vám riziko bezpečnostního incidentu podaří snížit na minimum. Zabezpečení však nikdy nemůže být dokonalé a je proto nezbytné, abyste měli zaveden plán okamžité reakce přizpůsobený potřebám Vašeho podniku, a díky tomu věděli, jaké kroky máte podniknout.

Pokud zjistíte porušení bezpečnosti ve Vašem podniku (únik dat), které se týká finančních dat z platebních karet, nebo pokud máte na takové porušení jen podezření, je nezbytné, abyste učinili následující opatření:

- okamžitě nás kontaktujte na následující emailové adrese: **pci@globalpayments.cz**

- nesnažte se o přístup nebo změnu narušených systémů – nepřihlašujte se do nich a neměňte žádná hesla

- nevypínejte tyto počítačové systémy: izolujte je od Vaší sítě a odpojte veškeré síťové kabely

- zachovejte veškeré logy generované počítačovými programy a obdobné digitální záznamy

- proveďte zálohu Vašich systémů, abyste je zachovali v současném stavu: usnadní to následné prošetření

- zaznamenejte podniknuté kroky

Vedle toho byste se měli obrátit s žádostí o profesionální poradenství na Kvalifikovaného forenzního vyšetřovatele schváleného PCI DSS. Seznam společností poskytujících tuto službu najdete na adrese: **www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php**

JAK OMEZIT FRAUDY/PODVODY

Podvody neboli fraudové transakce se staly globální epidemií, která ohrožuje všechny bez výjimky. Je lákavé domnívat se, že jakmile je platba autorizovaná, máte jistotu, že své peníze dostanete. Bohužel tomu tak není.

Autorizace nezaručuje platbu!

Když je poskytnuta autorizace, je tím potvrzeno pouze to, že na kartě jsou k dispozici potřebné finanční prostředky a že karta nebyla nahlášena jako ztracená či odcizená – zatím. Oprávněný vlastník nemusí vědět o tom, že někdo používá údaje o jeho platební kartě, a tak se transakce stále může ukázat jako podvodná.

Drtivá většina plateb kartou je dokončena bez jakéhokoliv problému. Avšak jen jedna jediná podvodná transakce může mít pro Vás významné negativní dopady: musíte jí věnovat čas, bude Vás stát peníze a může poškodit Vaši reputaci.

Podvodníci jsou vynalézaví, kreativní a přizpůsobiví. Abyste měli lepší povědomí o možných útocích podvodníků, sestavili jsme seznam nejčastějších podvodů, s nimiž jsme se v průběhu spolupráce s našimi zákazníky setkali.

TYPY PODVODŮ, NA NĚŽ JE TŘEBA SI DÁT POZOR

Použití několika karet a zamítnuté pokusy

Podvodníci si často kupují sady odcizených údajů z karet či tyto karty samotné a budou se snažit o objednávky po telefonu, faxem či online. Budou zkoušet každý soubor údajů z karet, dokud se nedostanou k údajům, které fungují. Pokud pozorujete několikanásobné zamítnutí, pak je u dané objednávky na místě ostražitost.

Požadavek na postoupení autorizace autorizačnímu centru

Pokud se na displeji Vašeho terminálu při provádění transakce objeví hláška jako „VOLEJTE AC nebo VOLEJTE HLAS. AUT.“, měli byste zavolat náš helpdesk (kontaktní údaje jsou uvedeny na str. 54), aby mohly být provedeny další kontroly, jejichž cílem je zjistit, že Váš zákazník je skutečným držitelem karty. Nikdy nepřijímejte autorizační kód, který Vám poskytne Váš zákazník, či kód od osoby, která zavolá Vaši firmu a tvrdí, že je z autorizačního centra. Kódy nejsou pravé a vydavatel karty bude schopen od Vás úspěšně reklamovat platbu, pokud takové kódy použijete.

Rozdělený prodej

Pokud dojde k zamítnutí transakce s celou částkou objednávky, nesnažte se celkovou sumu rozdělit do menších nebo ji rozdělit mezi více karet. Podvodníci si často nejsou vědomi zůstatku na kartě (kartách), které se jim dostaly do rukou, a budou po Vás chtít, abyste zadali různé částky, než transakce může projít.

Transakce prostřednictvím magnetického proužku a padělané karty

Transakce přes čip a PIN jsou ve světě stále častější, ale dokud nebude použití této technologie univerzálně rozšířené, stále bude potřeba mít na všech kartách magnetický proužek a pole pro podpis.

Pokud však karta čip má, buďte opatrní, říká-li zákazník, že čip nefunguje či že zapomněl své PIN.

Mějte se rovněž na pozoru před padělanými kartami, na něž byly vytištěny, vyraženy či zakódovány údaje ze skutečné karty. Většina padělaných karet je výsledkem podvodu, kterému se říká „skimming“, kdy jsou údaje z karty zkopírovány bez vědomí skutečného držitele karty. Ke „skimmingu“ dochází mj. na maloobchodních pokladnách, kde je karta umístěna do podvodného zařízení, které elektronicky kopíruje údaje držitele karty.

Je proto důležité, abyste při protahování karty čtečkou Vašeho terminálu dbali na dodržování pokynů v tomto dokumentu týkajících se kontrolování karet (viz str. 13).

Uvažte rovněž další níže uvedené varovné signály:

- mějte se na pozoru před zdánlivě náhodnými a nelogickými nákupy, jako když například zákazník nakoupí velké množství stejných kusů
- neobtěžoval se zákazník zkusit si oblečení?
- je zákazník nervózní a snaží se odvést Vaši pozornost?
- jde o transakci na nízkou částku s vysokou částkou Cashbacku?

- je částka transakce jen těsně pod Vaším autorizačním limitem?

Phishing

Phishing je způsob, jak mohou podvodníci získat údaje z karty, které následně mohou zneužít ke spáchání podvodu v prostřední CNP.

Phishing může být proveden pomocí emailů, které se tváří, že jsou od legitimní společnosti působící na internetu. Tyto emaily se snaží oklamat zákazníky a přimět je, aby uvedli citlivé informace na falešné internetové stránce vytvořené a provozované podvodníky. Tyto emaily obvykle tvrdí, že není třeba „aktualizovat" nebo „ověřovat" informace ze zákazníkova účtu a apelují na příjemce, aby klikli na odkaz v emailu, který je přesměruje na podvodnou stránku. Jakékoliv informace zadané na této stránce budou těmito zločinci zaznamenány a následně zneužity v jejich další kriminální činnosti.

Podvodníci rovněž mohou kontaktovat Vaši firmu a vydávat se technika opravujícího terminály nebo předstírat, že zastupují společnost Mastercard, Visa nebo Global Payments a vyžadovat informace o několika posledních transakcích, které jste zpracovali. **Nikdy** jim nedávejte žádné informace.

Pokud po Vás budeme požadovat jakékoliv informace, budeme s Vámi komunikovat z emailové adresy, která bude končit @fraudvgpe.cz. **Nikdy** však po Vás nebudeme chtít číslo karty.

V případě jakýchkoliv pochybností nás neváhejte prosím kontaktovat.

Emailové adresy

Existují dva typy emailových adres. Přístup k emailu je obecně součástí zákazníkova předplatného balíčku služeb od jeho Poskytovatele internetových služeb (ISP, Internet Service Provider). Případně mohou být užity „bezplatné" emailové účty, jako je například Yahoo, Hotmail nebo Google Gmail.

Řada zákazníků používá „bezplatné" emailové účty díky možnosti číst a posílat emaily kdekoliv, kde je internetové připojení. Nicméně podvodníci mají v oblibě právě „bezplatné" emailové účty, a to díky anonymitě, kterou jim poskytují – valná většina internetových podvodů byla spáchána tehdy, když podvodník uvedl „bezplatnou" emailovou adresu. Je na místě být podezřívavý, pokud není zákazníkovo jméno nějakým způsobem součástí emailové adresy.

Emailová adresa sama o sobě by neměla být podkladem pro rozhodnutí, zda transakce může být podvodná. Pokud je užita „bezplatná" emailová adresa, je třeba provést další formy ověření.

Doporučujeme zákazníkovi poslat email poté, co byla učiněna objednávka. Silně doporučujeme nepokračovat s transakcí, pokud Vám emailový program oznámí, že email nemohl být na adresu doručen.

Požadavek platit třetím stranám bankovním převodem

Buďte podezřívaví, pokud zákazník učiní objednávku na zboží a/nebo služby a zároveň Vás požádá, abyste přijali platbu za dodatečné služby, které má poskytnout jiná společnost. Poté jste zákazníkem požádáni, abyste tyto dodatečné peníze, které jste předtím převzali, přeposlali bankovním převodem oné druhé společnosti. Zákazník Vám může rovněž nabídnout dodatečnou sumu jako výraz díků za to, že jste mu pomohli. Jde však o podvod, který nejčastěji vídáme v hotelech a penzionech.

Rovněž buďte velmi opatrní v případě, že zboží vyvážíte do jiné země a Váš zákazník Vás požádá, abyste jeho přepravci bankovním převodem zaslali určitou finanční částku. Je možné, že přepravce neexistuje a objednávka je se značnou pravděpodobností podvodná.

Zamítněte veškeré požadavky, které případně dostanete, na převedení přeplatků třetím stranám, jako jsou prostředníci a facilitátoři, pomocí bankovního převodu.

Podvody s vracením peněz

Pokud je nákup proveden s jednou kartou, veškeré vrácení peněz by mělo být na tutéž kartu. Je na místě pojmout podezření, pokud zákazník žádá o vrácení peněz na jinou kartu nebo o vrácení prostřednictvím bankovního převodu.

Bohužel se často setkáváme s případy, kdy některý ze zaměstnanců zpracuje transakci s vrácením peněz tak,

že peníze vrátí na svou vlastní kartu – ujistěte se proto, že máte kontrolu nad tím, kdo má přístup k supervizorskému PIN k Vašemu terminály. Zajistěte, že máte zavedeny procedury, které Vám pomohou odhalit neobvyklou aktivitu v oblasti vracení peněz.

Rovněž byl v poslední době zaznamenán nárůst počtu podvodů, které využívají sociálně inženýrské techniky, jako je například phishing, k získání informací o účtu obchodníka s cílem provést podvodné vrácení peněz. S využitím takto získaných údajů jsou zločinci schopni nabourat se do obchodníkovy platební brány či do software dodaného třetí stranou a pak zadat vrácení peněz na účet karty, který byl předtím vytvořen s použitím falešných údajů nebo díky krádeži účtu. Jakmile jsou peníze připsány na účet, jsou rychle vybrány. Tyto transakce se mohou jevit, jako by byly na účty držitelů karet legitimně vráceny peníze za reklamované zboží, ale ve skutečnosti nikdy žádné zboží nebo služby nebyly nakoupeny.

Abyste snížili riziko, že se Vaše firma stane obětí tohoto typu podvodů, musíte vždy:

- zajistit, že vaše uživatelské jméno a heslo k účtu jsou uloženy v šifrované formě
- zajistit, že hesla pro internetové platební brány jsou pravidelně měněna – minimálně každých 90 dní
- při vracení peněz se ujistěte, že máte údaje k původní prodejní transakci a že peníze vracíte na ten samý účet spojený s kartou
- pokud vlastníte mobilní terminál, ujistěte se, že je za všech okolností zabezpečen, aby jej zločinci nemohli jednoduše vzít a odejít s ním
- pokud jste dostali nový terminál pro prodejní místo (POS), změňte si okamžitě heslo supervizora z továrně nastaveného náhodného kódu a toto heslo dále pravidelně měňte
- okamžitě nás informujte, pokud se Váš POS terminál ztratí či bude odcizen. To zajistí, že tato zařízení budou zablokována, aby s nimi nešlo dále zpracovávat platby

JAK MOHU OCHRÁNIT SVŮJ PODNIK?

Máme motivovaný a odhodlaný tým, jehož součástí jsou vyšetřovatelé podvodů, kteří využívají monitorovací nástroje k tomu, aby vyhodnocovali a monitorovali rizika podvodů. Tento tým prověřuje vzorce v obchodních transakcích obchodníka, aby stanovil, zda se objevila jakákoliv podvodná činnost či se k takové činnosti schyluje.

Výše zmíněné však nezpůsobí, že se žádné podvody dít nebudou. Budete muset zavést určité obchodní praktiky, díky nimž budete moci minimalizovat riziko podvodu a s ním spojených finančních ztrát.

Pokud zpracováváte CNP transakce, musíte být ještě více ostražití. S těmito transakcemi je spojeno ještě větší inherentní riziko, neboť nejste schopni zaručit, že informace jsou Vám poskytovány skutečným držitelem karty. Přijímání CNP transakcí tedy významně zvyšuje Vaši zranitelnost vůči podvodům, chargebackům a v konečném důsledku vůči finančním ztrátám. Je tomu tak proto, že nemůžete fyzicky ověřit transakci provedením ověřovacích kontrol a kontrolou podpisu a PIN držitele karty.

Pokud přijímáte CNP transakce, nebudete se těšit stejné ochraně jako zákazník, který provádí pouze transakce v osobním kontaktu se zákazníkem, a budete to Vy, kdo bude v budoucnu hradit chargebacky v případě jakéhokoliv sporu. Je dobrou praxí dále prošetřit, pokud se u CNP transakce objevily jakékoliv anomálie. Prošetřování může zahrnovat jak použití pro dané odvětví standardních nástrojů prevence podvodu, tak kontroly ověřující transakci z perspektivy „zdravého rozumu".

Nemějte obavy ze zamítání podezřelých objednávek. Nejste nijak zavázáni provést transakci, kterou považujete za podvodnou.

Nástroje prevence podvodů

Nástroje prevence podvodů, jako je například služba ověřování adres (AVS, Address Verification Code) a bezpečnostní kód karty (CSC) jsou vytvořeny k tomu, aby Vám pomohly s autentizací transakce. Na rozdíl od PIN nebo podpisu nepotvrzují AVS a CSC identitu držitele karty, ale pokud jsou užity současně, nabízejí další informace, které Vám pomohou rozhodnout se, zda transakci provést.

Bezpečnostní kód karty (CSC): CSC poskytuje další bezpečnostní informace, jejichž cílem je potvrdit, že zákazník má kartu fyzicky u sebe. Pokud je tento kód na kartě uveden, může se objevovat v podobě posledních tří číslic vytištěných na zadní straně karty na podpisovém proužku nebo v bílém políčku napravo od podpisového proužku. U karet American Express má toto číslo čtyři číslice a je vytištěno na přední straně karty.
Kód CSC může být nazýván rovněž CVV, CVV2 nebo CVC2.

Mastercard SecureCode (SecureCode)/Verified By Visa (VbV): U transakcí přes internet může být do internetových stránek implementována dodatečná bezpečnostní vrstva. Řešení SecureCode a VbV, která lze zahrnout pod souhrnný název 3D Secure, byla vyvinuta, aby umožňovala zákazníkům prokázat se jako skuteční držitelé karty.

SecureCode a VbV představují globální řešení pro internetové obchodní transakce, které držitelům karty umožňují prokázat se svým vydavatelům karty pomocí unikátního osobního kódu a hesla.

Držitel karty musí zadat své heslo ve zvláštním okně prohlížeče před tím, než může dojít k autorizaci jeho online transakce. Vydavatel karty potvrzuje, že jde o skutečného držitele, který momentálně provádí transakci. Držitel karty může být klidný, neboť ví, že nikdo jiný nemá přístup k jeho heslu, a Vy získáte explicitní doklad autorizovaného nákupu.

V případě, že musí být následkem podvodu při standardní online transakci proveden chargeback, obchodník je povinen zaplatit rozporovanou částku transakce. Užití 3D Secure může odpovědnost přenést z obchodníka na vydavatele karty. Odpovědnost je přenesena za následujících podmínek:

- obchodník a zpracovatel karty nainstalovali tuto službu, ale karta není pro službu registrována
- obchodník a držitel karty se zaregistrovali k užití této služby a držitel karty se prokáže jako skutečný držitel
- obchodník a zpracovatel karty nainstalovali 3D Secure službu, ale vydavatel karty nemá oprávnění službu provozovat

Abyste získali výhody, které přináší 3D Secure, budete muset na svých internetových stránkách zavést požadovanou technologii. Toho lze provést nahráním registrované aplikace Merchant Plug-In (MPI) na Váš server. Případně můžete uzavřít smlouvu s poskytovatelem hostované služby, aby za vás autentizační proces prováděl.

Provádění internetových transakcí bude čistě na Vaše vlastní riziko, nehledě na to, zda byly jakékoliv požadavky na autorizaci či jiné požadavky adresovány na nás.

Využití autentizačního procesu 3D Secure pro internetové transakce toto riziko snižuje. Proces je dostupný jen u karet Mastercard a Visa. Pokud je totožnost držitele karty úspěšně ověřena prostřednictvím SecureCode a/nebo VbV, nedojde k chargebacku čistě jen proto, že držitel karty zamítá provedení transakce. Toto rovněž platí, pokud je autentizace zahájena, ale nemůže být dokončena, protože se držitel karty, ať už z jakéhokoliv důvodu, neúčastní transakce se SecureCode nebo VbV.

Pokud identita držitele karty nemůže být ověřena z jakéhokoliv jiného důvodu, včetně selhání Vašeho vlastního zařízení z jakékoliv příčiny či jakékoliv chyby či opomenutí při zadávání dat, kterých jste se dopustili Vy nebo držitel karty, nebudete se těšit výše zmíněné ochraně před chargebackem. Proces autentizace a jeho dopad na odpovědnost za příslušnou transakci pokrývají příslušná pravidla Mastercard a Visa, která se čas od času mění. Tato pravidla mj. z autentizačního procesu vylučují určité karty a transakce. To znamená, že i pokud jste se rozhodli užívat 3D Secure, tato služba a ochrana, kterou nabízí, se nebude vztahovat na všechny transakce. Další informace naleznete na internetových stránkách Visa a Mastercad. Mějte prosím na paměti, že transakce může být reklamována a úhrada reklamované částky může být od Vás vyžadována z jakéhokoliv jiného důvodu.

Abyste mohli přes internet přijímat karty Maestro, musíte podporovat Mastercard SecureCode. Pokud nepodporujete SecureCode pro internetové transakce s kartou Maestro, vystavujete se tím riziku významného finančního postihu.

Testování zaměřené na odhalování podvodů

Pokud přijímáte CNP transakce, pak silně doporučujeme zavést systém testování zaměřený na odhalování

podvodů, který testuje platnost a historii karet předkládaných k provedení transakce.

Mezi tyto testy by měla patřit přinejmenším kontrola:

- adresy z výpisu
- země adresy z výpisu
- doručovací adresy
- telefonních čísel
- transakcí se stejnou hodnotou
- toho, kolikrát byla karta v daném časovém období použita

Vedle výše zmíněných kontrol rovněž důrazně doporučujeme provést následující kontroly zaměřené na odhalení podvodu u internetových transakcí:

- kontrolu lokace IP (Internet Protocol) adres vzhledem k zemi vydání karty/zemi, kde se nachází doručovací adresa
- prověření frekvence užívání a to, zda adresy nejsou spojeny s objednávkami z více jak jedné doručovací adresy
- prověření emailových adres, které je popsáno v sekci na str. 49

Deset tipů, jak předejít podvodům v prostředí CNP

Podvodům v prostředí CNP může pomoci zabránit vysoká ostražitost. Pokud mohou zaměstnanci prodeje na jednu nebo více z níže uvedených otázek odpovědět „ano“, neznamená to, že transakce je podvodná – znamená to však, že byste měli zvážit provedení dalších kontrol, než transakci dokončíte.

1. Je prodej příliš snadný? Nejeví zákazník zájem o cenu či detaily zboží? Jde o nového zákazníka? Nachází se adresa zákazníka v oblasti, kam běžně zasahují Vaše obchodní aktivity? Pokud ne, proč si pak objednává od Vás?
2. Má zboží vysokou hodnotu nebo je lze snadno přeprodat?
3. Je částka za prodej nadměrně vysoká v porovnání s Vašimi obvyklými objednávkami? Objednává si zákazník velké množství různých předmětů, nebo několik kusů toho samého předmětu? Liší se nějak od Vašeho obvyklého zákazníka?
4. Poskytuje zákazník údaje o kartě někoho jiného, například klienta nebo člena rodiny?
5. Je ochoten dát Vám jen číslo mobilního telefonu?
6. Vypadá adresa podezřele? Byla doručovací adresa užita již v minulosti s odlišnými údaji o zákazníkovi? Nachází se doručovací či kontaktní adresa v zahraničí? Jedná se o veřejně dostupné místo jako kavárna, čerpací stanice, chata atd.?
7. požaduje zákazník doručení na neobvyklé místo v určitém čase?
8. Dostává zákazník instrukce, co má dělat, od třetí strany, zatímco telefonuje nebo se zdá při odpovídání na určité otázky váhat?
9. Užívá zákazník více než jednu kartu k tomu, aby rozdělil celkovou částku za nákup?
10. Zdá se, že zákazník dostatečně nezná svůj účet?
11. Zdá se, že zákazník má potíže vzpomenout si na svou adresu bydliště a telefonní číslo? Zní zákazník, jako by četl z poznámek

DALŠÍ DŮLEŽITÉ INFORMACE

BUDEME VÁS PRŮBĚŽNĚ INFORMOVAT

Budeme Vám zasílat pravidelné aktualizace o záležitostech, které ovlivňují způsob, jakým přijímáte a zpracováváte transakce s kreditními a debetními kartami.

Je velmi důležité, abyste si tyto aktualizace přečetli a řídili se našimi doporučeními, zvláště těmi, která se týkají povinných změn vyžadovaných provozovateli sítě platebních karet. Prosím kontaktujte nás v případě, že potřebujete další pomoc nebo podporu (kontaktní údaje jsou uvedeny na str. 54) či pokud máte obavy, že tyto informace nedostáváte.

PAPÍROVÉ KOTOUČKY PRO ELEKTRONICKÉ TERMINÁLY

Pokud provozujete elektronický terminál, ujistěte se, že máte dostatek papírových kotoučků.

Pro objednání papírových kotoučků prosím zavolejte Vašemu dodavateli kancelářského vybavení, protože my sami papírové kotoučky našim partnerům z řad obchodníků neposkytujeme. Vždy se ujistěte, že objednáváte správný typ pro Váš platební terminál.

TVORBA VAŠÍ VLASTNÍ REKLAMY

Pokud chcete vytvořit své vlastní materiály, v nichž budete zákazníkům sdělovat, že přijímáte platební karty jako způsob úhrady, požádejte nás prosím o náš balíček relevantních obrazových materiálů.
Tento balíček poskytuje detailní informace o tom, jak reprodukovat loga provozovatelů sítě platebních karet. Mějte prosím na paměti, že platí následující pravidla:

- loga karet byla registrována jako ochranné známky a musí být užívána v souladu s instrukcemi obsaženými v balíčku obrazových materiálů

- loga karet nesmí být užita v reklamě způsobem, který by naznačoval, že provozovatelé sítí platebních karet propagují Vaše služby nebo zboží

- jste povinni předložit nám ke schválení veškeré propagační nebo prodejní materiály, v nichž je zmíněna naše společnost či karta jakéhokoliv typu

- vaše stránka pro internetovou platbu musí obsahovat příslušná loga provozovatelů sítí platebních karet

Dále, pokud si přejete užít logo Global Payments na své internetové stránce či v reklamním materiálu, musíte uzavřít Licenční dohodu o ochranné známce. Kontaktujte nás prosím, přejete-li si získat více informací (kontaktní údaje jsou uvedeny na str. 54).

Každá Vaše prodejna a její prodejní místo musí být v příslušném propagačním materiálu jasně identifikována.

JAK NÁS KONTAKTOVAT

Mějte připraveno Vaše číslo obchodníka, kdykoliv nás telefonicky kontaktujete. Toto číslo je uvedeno na účtenkách z elektronických terminálů.

Hovory jsou čas od času monitorovány a zaznamenávány za účelem zlepšení naších služeb, které Vám poskytujeme. Jakékoliv nahrávky zůstávají výhradně v našem vlastnictví.

HELPDESK/NONSTOP ZÁKAZNICKÁ LINKA GLOBAL PAYMENTS

Dostupná 24 hodin denně, 7 dní v týdnu, 365 dní v roce
+ 420 267 197 777
helpdesk@globalpayments.cz

Jsme tu proto, abychom Vám pomohli, proto nám neváhejte zavolat či poslat email.

Nebo nám napište na: Global Payments s.r.o., centrála
V Olšinách 80/626
100 00 Praha 10 – Strašnice
Česká republika

POKUD CHCETE VZNÉST STÍŽNOST

Pokud z jakéhokoliv důvodu nejste v některém ohledu spokojeni s našimi službami, chceme se s Vámi co nejdříve spojit. Poté vzneseme příslušné dotazy a pokusíme se celou záležitost napravit, jakmile to bude možné.

Začněte prosím tím, že zavoláte naši zákaznickou linkua sdělíte nám, kde vznikl problém. Pokusíme se na Vaši stížnost odpovědět ihned, a pokud tak nebudeme schopni učinit, záležitost dále prošetříme a jakmile budeme moci, zavoláme Vám zpět.

Pokud budete mít poté pocit, že jsme problém nevyřešili k Vaší spokojenosti, můžete svou stížnost prostřednictvím naší zákaznické linky eskalovat nebo můžete napsat na naše ústředí sídlící na adrese:

Global Payments s.r.o.
V Olšinách 80/626
100 00 Praha 10 – Strašnice
Česká republika
Email: info@globalpayments.cz

Global Payments s.r.o.
V Olšinách 626/80
Praha 10 - Strašnice
100 00

Tel.: +420 267 197 191
Telefonní linka je dostupná od pondělí do pátku od 9.00 do 17.00, kromě státních svátků.

Ve spolupráci s

globalpayments

ČESKÁ SPOŘITELNA

globalpaymentsinc.com

SERVICE. DRIVEN. COMMERCE

Global Payments je obchodní firmou společnosti Global Payments s.r.o., která podniká v České republice, se sídlem V Olšinách 626/80, Strašnice, 100 00 Praha 10, Česká republika, IČO: 042 35452 zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl C, vložka 244453. Global Payments s.r.o. je autorizována Českou národní bankou na základě zákona č. 284/2009 Sb., o platebním styku a podléhá regulaci