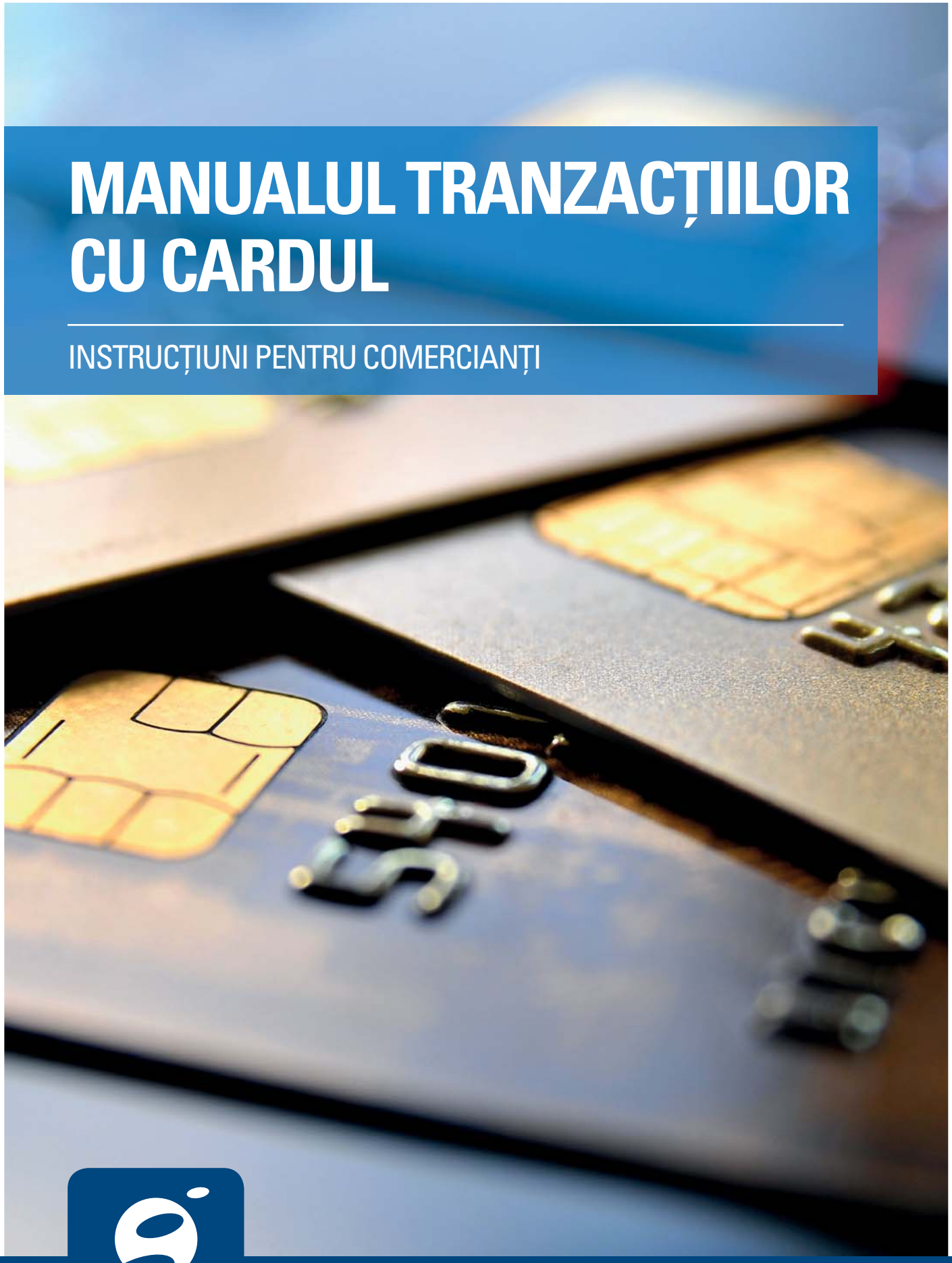
MANUALUL TRANZACȚIILOR CU CARDUL

INSTRUCȚIUNI PENTRU COMERCIANȚI



SERVICE. DRIVEN. COMMERCE

globalpaymentsinc.com

CUPRINS

BINE AȚI VENIT!

Ne bucurăm că ați devenit clientul societății Global Payments al cărei scop unic și simplu este de a vă oferi servicii sigure și fiabile în domeniul procesării tranzacțiilor cu cardul.

Aceasta înseamnă o colaborare strânsă cu Dumneavoastră.

Ascultăm cu atenție ceea ce ne spuneți despre necesitățile Dumneavoastră, iar acest lucru ne ajută să înțelegem amănunțit afacerea Dumneavoastră. Ne vom strădui să colaborăm cu Dumneavoastră în mod profesional, transparent și corect. Părerea Dumneavoastră privind serviciile noastre este importantă pentru noi, vom fi bucuroși să o împărtășim împreună.

DESPRE NOI

La data de 1 iunie 2016, societățile Global Payments Inc., prestator de top, la nivel mondial, de servicii în domeniul tehnologiilor pentru procesarea plăților, CaixaBank, cea mai mare bancă spaniolă, conform cotei de piață și Erste Group, prestator marcant de servicii financiare din Europa centrală și de est, au încheiat un parteneriat pentru oferirea serviciilor de plată prin card comerciantilor din Republica Cehă, Slovacia și România.

Rezultatul Contractului l-a constituit înființarea societății independente cu personalitate juridică, sub denumirea de Global Payments s.r.o. care funcționează independent de societatea Global Payments Europe, s.r.o. (GPE), partenerul nostru în domeniul tehnic, în domeniul inovațiilor și în prestarea serviciilor de asistență pentru comercianți.

Societatea Global Payments își dezvoltă soluțiile sale pe baza necesităților clienților de pe întreg globul și este partenerul căutat datorită faptului că oferă un portofoliu extins de produse și servicii care îi ajută pe clienții săi să crească și să inoveze. Fie că că este vorba de plăți în persoană, online sau „ în mers", întotdeauna vă oferim asistența noastră tehnică în căutarea și implementarea soluțiilor unice în domeniul serviciilor de plată.

În calitate de societate care se axează pe servicii și comerț, Global Payments depune eforturi maxime pentru a fi un membru responsabil al comunității, iar angajații noștri dau dovadă de pasiune și entuziasm pentru schimbările pozitive din viața celorlalți. Facem parte din comunitatea globală de afaceri și relația noastră cu aceasta este importantă pentru valorile pe care le deține societatea noastră și pentru ceea ce suntem: în întreaga lume ne străduim să contribuim la schimbările pozitive, oferind timpul nostru, serviciile și asistența financiară persoanelor care au nevoie de aceasta.

DESPRE SOCIETATEA GLOBAL PAYMENTS

Global Payments Inc. este prestatorul de top la nivel mondial în domeniul serviciilor de plată, furnizând soluții inovative adaptate clienților de pe tot globul. Tehnologia noastră, partenerii și competența profesională a angajaților noștri ne dau posibilitatea să livrăm un pachet extins de produse și servicii, astfel încât clienții noștri să poată beneficia de toate instrumentele din domeniul acceptării și procesării plăților prin intermediul cardurilor de plată între diferitele canale de distribuție din multe medii de piață de pe tot globul.

Societatea Global Payments, cu sediul în Atlanta (statul Georgia, SUA), are peste 8500 de angajați pe tot globul, este încadrată în lista S&P 500 și are parteneri și clienți în 30 de țări din toată America de Nord, Europa, regiunea Asia-Pacific și în Brazilia. Pentru mai multe informații despre societatea Global Payments, cu marca Service. Driven.Commerce și tehnologiile ei, vă rugăm să vizitați site-ul www.globalpaymentsinc.com.

DESPRE ACEST DOCUMENT

Aceste Instrucțiuni pentru comercianți, împreună cu celelalte documente menționate la punctul 1.1. din Condițiile comerciale generale reprezintă Contractul de acceptare a cardurilor de plată pe care îl veți încheia cu noi (denumit în continuare „Contractul").

În interesul nostru comun ar trebui să citiți cu atenție acest document, întrucât constituie parte integrantă a Contractului pe care intenționăm să ne bazăm. Dacă nu înțelegeți vreun punct, vă rugăm să solicitați detalii. Datele noastre de contact se găsesc la pagina 52.

Ce puteți afla din acest manual pentru comercianți?

Acest manual vă oferă:

- o imagine de ansamblu asupra diferitelor moduri prin care putem să promovăm compania Dumneavoastră
- informații privind factura noastră și alte instrucțiuni de utilizare

- informații importante privind riscurile legate de utilizarea și acceptarea cardurilor; manualul prezintă sugestii și sfaturi utile pe care este important să le respectați pe parcursul acceptării cardurilor de plată

- manualul vă oferă posibilitatea să efectuați eficient și în deplină securitate tranzacții cu cardul

Vă rugăm să citiți cu atenție acest document: cuprinde informații cheie care vă pot ajuta pentru prevenirea fraudelor și chargeback-urilor *(refuzurile la plată)*.

Vă rugăm să respectați cu temeinicie procedurile descrise detaliat în acest manual. Datorită acestora, Dumneavoastră și compania Dumneavoastră veți putea optimiza acceptarea la plată a cardurilor .

De asemenea, ar trebui să aveți la dispoziție, într-un loc adecvat, o copie după aceste Instrucțiuni pentru comercianți pentru a vă putea fi ușor accesibile, în caz de nevoie, Dumneavoastră și angajaților Dumneavoastră. Dacă nu veți putea găsi informațiile de care aveți nevoie, vă rugăm să ne contactați (vizitați pagina 52 unde sunt menționate datele de contact).

Vă rugăm să ne informați despre schimbările din activitatea Dumneavoastră comercială.

De acceptarea la plată a cardurilor sunt legate și riscurile și noi considerăm că este obligația noastră să ne asigurăm că sunteți conștienți de aceste riscuri. Vă vom informa despre evoluția din acest sector, inclusiv despre tendințele din activitatea frauduloasă și progresele din procesele și tehnologiile orientate asupra luptei împotriva fraudelor. Astfel vă vom ajuta să menținem securitatea la nivelul cel mai înalt posibil și să reducem riscul care amenință afacerea Dumneavoastră.

Pentru a putea să vă oferim informații actuale și să vă asigurăm că primiți serviciile corespunzătoare, vă rugăm să ne anunțați dacă se modifică vreuna din datele menționate mai jos privind afacerea Dumneavoastră, spre exemplu:

- Datele Dumneavoastră de contact (inclusiv adresa de email și numărul de telefon);
- Adresa Dumneavoastră (inclusiv sediul Dumneavoastră comercial, adresa de corespondență, adresa sediului Dumneavoastră central ș.a.m.d.);

- Tipul de afacere căreia vă dedicați;

- Schimbări importante în numărul de tranzacții comerciale pe care le efectuați;

- Intenționați să schimbați modul în care desfășurați activitatea, spre exemplu, dacă apreciați că veți începe să faceți tranzacții pe Internet sau veți începe să utilizați serviciile unui nou Prestator de servicii de plată (PSP, Payment Services Provider);

- Schimbări importante în participațiile la capitalurile proprii din societatea Dumneavoastră (de regulă se consideră importantă și schimbarea referitoare la mai mult de 25% cotă-parte); sau

- Dacă vindeți compania Dumneavoastră sau dacă îi schimbați forma juridică.

Pentru a ne informa referitor la orice schimbare din cele menționate mai sus, vă rugăm să folosiți linia noastră pentru clienți (vizitați pagina 52 unde sunt menționate datele de contact) sau formularul privind schimbarea care este disponibil spre descărcare pe Portalul Comerciantului (Merchant Portal).

Vă rugăm să nu ezitați să ne contactați pentru orice fel de întrebări sau pentru feedback.

Scopul nostru este să vă oferim servicii de cea mai bună calitate posibilă. De aceea salutăm orice fel de observații și feedback-ul. Vă rugăm să nu ezitați să ne contactați dacă aveți orice fel de întrebări sau observații referitoare la aceste instrucțiuni sau orice aspect al serviciilor oferite de noi. Datele de contact le găsiți la pagina 52.

DEFINIREA UNOR NOȚIUNI

SA
Service autorizat – locul unde sunt realizate cerințele de autorizare a plăților.

ORGANIZAȚII DE CARDURI
Organizație internațională care acordă băncilor licențe pentru emiterea și prelucrarea tranzacțiilor realizate cu cardurile de plată (Visa Intl., Mastercard Intl., Diners Club Intl., Japan Credit Bureau Intl., American Express Intl.).

AUTORIZARE
Proces de verificare a posibilității de a realiza plata prin intermediul cardului de plată. Servește pentru verificarea valabilității cardului și aprobarea tranzacției cu cardul.

COD DE AUTORIZARE
O combinație din patru până la șase cifre (la organizația American Express este doar din două) sau de cifre și litere care i se comunică partenerului de afaceri ca referință a autorizării favorabile emise prin efectuarea tranzacției cu cardul.

LIMITĂ DE AUTORIZARE
Valoarea maximă (stabilită implicit la 0,00 RON) la care tranzactia se poate realiza prin intermediul unui singur card de plată, într-un singur loc de tranzacționare a Comerciantului pe parcursul unei zile calendaristice, fără a fi strict necesar să se solicite autorizarea pentru tranzacția cu cardul prin intermediul SA. Valoarea sumei poate fi modificată pentru unele segmente, pe baza cererii trimise către PPS.

TEHNOLOGIE CONTACTLESS (FĂRĂ CONTACT)
Acceptarea contactless a cardurilor de plată. La plățile contactless, pe cardul de plată este reprezentat, în afară de elementele standard de securitate și simbolul care îi autorizează pe titularii de card să efectueze tranzacții contactless.

CITITOR CONTACTLESS (FĂRĂ CONTACT)
Dispozitivul cititor contactless, dispus în afara terminalului de plată sau parte componentă a terminalului de plată, conceput pentru acceptarea cardurilor de plată și a celorlalte dispozitive cu tehnologie contactless.

CIP
Microprocesorul dispus pe partea frontală a cardului de plată. Arată ca o suprafață metalică, sub formă ovală sau dreptunghiulară.

DCC
Conversia valutară dinamică (Dynamic Currency Conversion), aplicație pentru POS care îi permite titularului de card opțiunea de a plăti pentru bunuri sau servicii, în moneda din țara de origine.

TITULAR DE CARD
Persoana fizică, rezidentă sau nerezidentă, căreia i-a fost emis cardul de plată, pe baza contractului încheiat cu emitentul cardurilor de plată și ale cărei prenume și nume sunt marcate pe cardul de plată.

CARD DE PLATĂ HIBRID
Cardul de plată care conține în sine mai multe aplicații de plată ale unei organizații de carduri (spre exemplu, Cardul Visa de debit și de credit) sau poate să conțină mai multe marcaje de plată ale organzațiilor de carduri.

MASTERCARD MOBILE
Portofelul de plată electronică din telefonul mobil al clientului

MPOS
Dispozitiv mobil pentru acceptarea electronică și procesarea (banda magnetică sau CIP-ul) tranzacțiilor cu cardurile cu contact și contactless

TEHNOLOGIE NFC
NFC (Near Field Communication) este tehnologia wireless (fără fir) – transmiterea datelor prin radio, la distanță scurtă, care permite comunicarea bidirecțională simplă și sigură între dispozitivele electronice, cum sunt efectuarea tranzacției contactless, spre exemplu, cu telefonul mobil, brelocul, ceasul, sticker-ul, plata prin codul QR ș.a.m.d.

LOCUL DE TRANZACȚIONARE/PUNCTUL DE VÂNZARE (POS-ul)
Locul în care sunt acceptate de Comerciant plățile prin intermediul cardurilor de plată/NFC pentru bunurile și serviciile oferite, adresa unde se află spațiile Comerciantului și unde a fost inițiată tranzacția respectivă de plată. Cu toate acestea, a) în cazul contractelor încheiate la distanță, în temeiul art. 2 punctul 7 din

directiva 2011/83/UE, punctul de vânzare este adresa sediului permanent al activității comerciale unde Comerciantul prestează activitatea sa, fără a ține cont de postarea paginilor de Internet sau de server și prin intermediul căreia tranzacția de plată este inițiată;
b) dacă Comerciantul nu are un sediu permanent de activitate, punctul de vânzare este adresa, în raport cu care Comerciantul are valabilă autorizația de funcționare prin intermediul căreia tranzacția de plată este inițiată;
c) dacă Comerciantul nu are un sediu permanent de activitate și nici nu are valabilă autorizația de funcționare, se consideră ca punct de vânzare (POS-ul), adresa de corespondență care este stabilită în scopul plății impozitelor legate de activitatea lui comercială și prin intermediul căreia tranzacția de plată este inițiată.

DESERVIREA LOCULUI DE TRANZACȚIONARE
Persoana fizică autorizată de Comerciant pentru acceptarea cardurilor de plată și pentru deservirea dispozitivelor respective (POS) de acceptare a cardurilor de plată.

PIN pad
Dispozitiv extern pentru introducerea PIN-ului care funcționează independent sau este cuplat la terminalul de plată.

PLATA CU CARDUL
Tranzacția cu cardul efectuată în folosul Comerciantului pentru achitarea bunurilor achiziționate sau a serviciilor prestate prin intermediul cardului de plată sau dispozitivului NFC.

CARD DE PLATĂ
Cardul din plastic care, prin aspectul său, prin dispunerea informațiilor și prin elementele de protecție, corespunde, pe fata și verso, specificației stabilite de organizația de carduri. Prin intermediul cardului de plată se pot realiza plățile fără numerar pentru bunuri și servicii și retragerea de numerar.

TERMINAL DE PLATĂ POS
Terminalul de plată electronică pentru acceptarea electronică și procesarea (banda magnetică și CIP-ul) tranzacțiilor cu cardurile cu contact și contactless. O parte componentă a acestuia poate fi și dispozitivul auxiliar pentru introducerea PIN-ului, așa-numitul PIN pad.

VALABILITATEA CARDULUI
Perioada pe parcursul căreia titularul cardului de plată poate beneficia de realizarea tranzacțiilor cu cardul. Valabilitatea cardului este marcată pe partea frontală a cardului de plată.
DOCUMENTAȚIA PENTRU TRANZACȚIE
Denumirea generală dată pentru toate documentele referitoare la tranzacție.

PRESTATORUL SERVICIILOR DE PLATĂ/PPS
Acquirer/Acceptant – furnizorul serviciilor de plată care încheie cu Comerciantul contractul privind acceptarea la plata cardurilor și furnizează servicii legate de acceptarea cardurilor de plată.

DOCUMENT DE VÂNZARE
Documentul pe suport de hârtie sau în format electronic privind efectuarea tranzacției cu cardul.

ACT DE IDENTITATE
Cartea de identitate, pașaportul sau permisul de ședere.

RAMBURSARE
Tranzacția efectuată în folosul titularului de card prin care Comerciantul se obligă să ramburseze plata prin intermediul PPS, Titularului de card, pentru bunurile reclamate sau rambursate.

INTRODUCERE ÎN PROCESAREA PLĂȚILOR CU CARDUL

Acceptarea cardurilor poate să aducă o serie de avantaje afacerii Dumneavoastră, inclusiv:

- îmbunătățirea fluxului de numerar
- oferirea unei metode alternative de plată
- oferte extinse de produse, cum este, spre exemplu, serviciul DCC

Societatea Global Payments va colabora strâns cu Dumneavoastră în căutarea acelei soluții corecte în domeniul procesării tranzacțiilor cu cardul pentru activitatea Dumneavoastră comercială și care reprezintă un serviciu de calitate la un preț cât mai avantajos pentru Dumneavoastră.

Dacă în domeniul procesării tranzacțiilor cu cardul de plată vă hotărâți să beneficiați de serviciile societății Global Payments, noi ne vom strădui permanent să dezvoltăm afacerea Dumneavoastră care utilizează tocmai serviciile noastre, să reducem numărul de situații în care este necesar să rambursați banii pentru tranzacția reclamată (așa-numitul chargeback) și să minimizăm costurile asociate management-ului plăților în numerar.

TIPURI DE TRANZACȚII

Serviciile în domeniul merchant acquiring-ului – de acceptare și procesare a tranzacțiilor realizate cu cardul vă dau posibilitatea de a accepta aceste forme de plată din partea clienților și acestea se pot împărți în două grupe de bază, conform tipului de tranzacții:

Tranzacțiile în care cardul este prezent (CP, Card Present), ceea ce înseamnă toate tranzacțiile în care cardul și titularul lui sunt fizic prezenți în momentul tranzacției și unde puteți să vă convingeți de prezența cardului prin citirea CIP-ului, prin trecerea benzii magnetice a cardului cu cititorul sau prin aplicarea la terminalul electronic. Cuprinde următoarele tipuri de tranzacții:

- tranzacții de vânzare referitoare la vânzarea de bunuri sau servicii
- cumpărarea prin retragerea de numerar („cash back", posibilă doar la cardurile de debit) – tranzacțiile legate de vânzarea de bunuri sau servicii, când totodată clientul primește înapoi și o sumă numerar

Tranzacțiile în care cardul nu este prezent (CNP, Card Not Present), ceea ce înseamnă tranzacțiile când cardul și titularul de card nu sunt fizic prezenți în momentul tranzacției. Această grupă cuprinde următoarele tipuri de tranzacții:

- tranzacția de vânzare cu comandă prin poștă, telefonic sau cu ajutorul altui tip similar de comunicare
- tranzacțiile realizate prin Internet
- tranzacțiile recurente (doar la anumite tipuri de carduri), când titularul de card vă autorizează pentru reținerea unor sume fixe sau variabile, în anumite intervale de timp (care pot fi specificate dinainte) de pe cardul Dumneavoastră și care includ abonamentele, reînnoirea calității de membru și plățile periodice

Mai există și alte tipuri de tranzacții care pot fi de tipul CP sau de tipul CNP, spre exemplu, tranzacțiile în câteva valute, în care, acest manual pentru comercianți vă oferă instrucțiunile cum să le acceptați pe acestea, la fel ca și plățile menționate mai sus.

În Cererea de acceptare a cardurilor de plată (denumită în continuare ‚Cererea') veți găsi descrierea detaliată a tipurilor de tranzacții și a tipurilor de carduri pentru care aveți autorizarea de acceptare. Pentru procesarea altor tipuri de tranzacții sau pentru acceptarea altor tipuri de carduri față de cele care sunt menționate în Cererea Dumneavoastră, trebuie să aveți autorizarea noastră în scris.

CONȘTIENTIZAREA RISCURILOR

Dorința noastră este ca societatea Dumneavoastră să poată accepta cardurile fără niciun fel de probleme. Este esențial să fiți foarte conștienți și să înțelegeți riscurile legate de acceptarea cardurilor.

Unul dintre aceste riscuri este așa-numitul chargeback (rambursarea sumei tranzacției pe cardul clientului), ceea ce înseamnă tranzacția cu cardul reclamată care ne-a fost rambursată de emitentul cardului. Este posibil să vă retragem suma reclamată din contul Dumneavoastră – cu

toate acestea, această secțiune descrie unele metode prin care puteți minimiza acest risc pentru activitatea Dumneavoastră comercială.

Nu există nicio garanție de rambursare a oricărei tranzacții, chiar dacă ați primit autorizarea. Autorizarea certifică faptul că, în momentul tranzacției, cardul nu este raportat ca fiind pierdut sau furat și că adevăratul titular de card dispune de fonduri suficiente pentru efectuarea tranzacției.

Nu acceptați niciodată ca valoarea achiziției să fie achitată cu mai mult de un card de plată și nu împărțiți niciodată tranzacția de vânzare în mai multe sume mai mici.

Tranzacțiile în care cardul este prezent (Tranzacțiile CP)

Cardul cu CIP care solicită PIN-ul

Tranzacția efectuată cu cardul cu CIP care solicită PIN-ul reprezintă în prezent una dintre cele mai sigure metode de plată cu cardul de plată. Toate tranzacțiile CP în care clientul solicita să plătească cu cardul cu CIP cu PIN, trebuie să fie efectuate cu ajutorul terminalului care permite citirea CIP-ului și introducerea PIN-ului.

După introducerea cardului cu CIP în terminal, la terminalul de plată sau la PIN pad se afișează suma tranzacției, titularul de card este invitat pentru confirmarea sumei prin introducerea PIN-ului, eventual titularul poate fi invitat mai întâi pentru confirmarea sumei și introducerea ulterioară a PIN-ului.

În cazul în care terminalul Dumneavoastră electronic nu are capacitatea de a citi informațiile înregistrate în CIP, va trebui să efectuați verificarea prin banda magnetică de pe card.

Cardul cu CIP care solicită semnătura

Există și carduri cu CIP care, în cazul introducerii lor în terminal, în loc de introducerea PIN-ului, solicită semnătura titularului de card. În acest caz, terminalul de plată tipărește chitanța cu rândul destinat pentru semnătura titularului de card. În continuare, procedați conform instrucțiunilor de la terminalul de plată.

Tranzacțiile contactless

Terminalul Dumneavoastră este dotat cu cititorul pentru acceptarea plăților contactless. Pe terminalul de plată sau la PIN pad se afișează suma tranzacției și titularul de card apropie cardul pe cititor, urmând a fi efectuată plata. Dacă nu este posibil să se efectueze plățile contactless cu cardul sau eventual cu terminalul sau dacă titularul de card acordă prioritate citirii CIP-ului și introducerii PIN-ului, se poate finaliza tranzacția prin introducerea cardului în cititor și prin introducerea PIN-ului.

În unele situații, terminalul Dumneavoastră poate solicita să fie efectuată tranzacția prin introducerea PIN-ului, în locul tranzacției contactless. Este vorba de funcția de securitate suplimentară al cărei scop este de a confirma faptul că titularul de card este proprietarul cardului. În acest caz este necesar să se continue pe calea obișnuită cu citirea CIP-ului cardului și prin introducerea PIN-ului.

Tranzacțiile cu bandă magnetică

În circulație există permanent o serie de carduri valabile care nu sunt prevazute cu CIP caz in care cardul va fi procesat prin citirea benzii magnetice.

În cazul în care tranzacția este efectuată prin banda magnetică, ca urmare a problemelor cu CIP-ul, este necesar să acordați atenție sporită, întrucât CIP-ul ar putea fi manipulat intenționat, pentru a nu fi nevoie să se facă verificarea prin intermediul PIN-ului.

În aceste situații tranzacția va fi autorizată online și depinde de Dumneavoastră să verificați ca semnătura de pe chitanță să fie conformă cu semnătura de pe card. Vă rugăm să procedați conform instrucțiunilor menționate la pagina 13 (Verificarea cardurilor). De asemenea este necesar să păstrați în siguranță o copie după chitanța semnată.

Tranzacțiile introduse prin tastatura de pe terminal

Pentru această posibilitate este necesar să aveți activată la terminal funcția „Introducere manuală". În caz contrar nu este posibil să se efectueze introducerea manuală a numărului cardului. Dacă vă interesează activarea acestui serviciu, vă rugăm să contactați centrul nostru de asistență.

La efectuarea acestui tip de tranzacție, procedați conform instrucțiunilor menționate în Manualul utilizatorului pentru terminalul Dumneavoastră de plată.

Tranzacțiile CNP (card not present)

Aceste situații sunt ideale pentru autorii fraudelor, întrucât cardul de plată, semnătura și codul personal de identificare (PIN-ul) nu pot fi verificate, deoarece este vorba de situația când Dumneavoastră, cardul și titularul de card **nu sunteți** prezenți împreună. Majoritatea tranzacțiilor reclamate (chargebacks-urile) se referă la tranzacțiile care au fost efectuate în mod fraudulos. Dacă încheiați o tranzacție despre care aveți îndoieli, o veți face pe propriul dumneavoastră risc. Consultați pag. 9 pentru mai multe informații privind tranzacțiile CNP.

Pentru a minimaliza riscurile legate de tranzacțiile CNP:

- Acordați o grijă sporită atunci când comanda a venit de pe un cont de email în care nu este inclus numele clientului, într-un fel sau altul, în adresa de email.

- Să fiți suspicioși față de tranzacțiile care sunt neobișnuit de mari, ținând cont de tipul afacerii Dumneavoastră, atât ca valoare, cât și ca volum, eventual vânzarea este „prea ușoară". Experiența noastră ne spune că tocmai la asemenea tranzacții este probabilitatea crescută că vor fi frauduloase.

- Dacă restituiți banii, întotdeauna să-i restituiți cu același card de plată cu care a fost efectuată tranzacția inițială.

- Țineți o bază de date a tranzacțiilor reclamate (chargebacks-urile) pentru a putea depista mai ușor formulele tranzacțiilor frauduloase. Dacă vânzarea pare să fie „prea bună pentru a fi adevărată", atunci este evident că nu este reală. Nu vă fie teamă să-i contactați pe titularii de card să le puneți întrebări suplimentare sau să solicitați identificarea suplimentară. Un client cinstit ar trebui să aprecieze că este vorba de securitate și că vă străduiți să vă protejați clienții Dumneavoastră împotriva fraudelor.

- Pentru tranzacțiile în cadrul comerțului online ar trebui să mai fie implementat pe site-uri încă un nivel de asigurare. Funcțiile Mastercard SecureCode și Verified by Visa (VbV) au fost create pentru a le permite clienților să facă dovada calității de adevărat titular al cardului.

- Trimiteți întotdeauna bunurile, recomandat sau prin poșta specială, sau prin intermediul unui transportator demn de încredere și sigur. Insistați asupra faptului că trebuie să fie emis documentul de înmânare care trebuie să fie ulterior semnat, dacă se poate, de către titularul de card. Solicitați curierului să nu transmită coletul, dacă spațiile unde se trece locul înmânării sunt goale. Vă rugăm să rețineți că documentul de plată în această formă nu constituie o probă suficientă care v-ar proteja pe Dumneavoastră împotriva tranzacției reclamate (chargeback-ul).

- Să nu transmiteți niciodată bunurile terților, cum sunt, spre exemplu, șoferii de taxi sau mesagerii.

- Acordați o grijă sporită tranzacțiilor în care adresa de facturare este diferită de adresa de înmânare solicitată. Evitați înmânarea la adresele care sunt diferite de adresele titularului de card, cum sunt, spre exemplu, hotelurile, cafenelele Internet și adresele altor persoane, unde își are reședința destinatarul.

- Procedați cu grijă în cazul cerințelor de livrare a doua zi, cerințelor pentru schimbarea rapidă a adresei de înmânare și la apelurile telefonice în ziua primirii în care cumpărătorul solicită un anumit timp de primire.

- Dacă clientul solicită ridicarea bunurilor din magazin, efectuați tranzacția la ridicarea bunurilor cu ajutorul dispozitivului Dumneavoastră pe care îl aveți la punctul de vânzare.

Mai multe informații despre modul în care trebuie să vă protejați afacerea Dumneavoastră, găsiți la pagina 55.

Dacă tranzacția a fost marcată ca frauduloasă și a fost recunoscut chargeback-ul, va trebui să rambursați înapoi suma achitată pe cardul clientului. Deci, se poate întâmpla să vă debităm din cont valoarea tranzacției. În cazul oricărei suspiciuni, sunați la centrul nostru de asistență și ca dovadă a autorizării comunicați-i „codul 10" (pagina 52).

Rețineți faptul că autorizarea nu este garanția plății.

Copie după documentul de vânzare

Oricând societatea noastra va poate solicita o copie după documentele de vânzare. Pentru orice fel de asemenea cerere vă rugăm să reacționați fără întârziere nejustificată, întrucât, în caz contrar, se poate ajunge la chargeback.

Păstrați întotdeauna în siguranță copia după documentele de vânzare în cadrul propriei dumneavoastră evidențe. Vă rugăm să rețineți că ar trebui să păstrați toate documentele privind tranzacțiile pe o perioadă de 24 luni de la primirea bunurilor sau încetarea serviciului prestat (consultați pagina 41 pentru informații detaliate privind securitatea datelor)

Securitatea datelor

În prezent cresc temerile privind securitatea datelor. Hoții caută noi căi de a obține aceste informații din diferite surse. O cale vulnerabilă prin care autorii fraudelor au reușit să le găsească o constituie informațiile financiare de pe cardurile de plată care sunt colectate pe parcursul procesării tranzacțiilor. Operatorii rețelelor cardurilor de plată au implementat un standard cu denumirea de *the Payment Card Industry Security Standard* (PCI DSS) care reprezintă un standard obligatoriu la nivel global cu scopul de a crește asigurarea acestui tip de date.

La acceptarea tranzacțiilor efectuate cu cardul de plată este necesar să conștientizați valoarea datelor pe care o colectați de la client, dacă efectuați tranzacția și de asemenea necesitatea de a proteja aceste informații. Dacă s-a produs un incident de securitate, vă expuneți unui risc substanțial de pierderi financiare și la prejudicierea reputației firmei Dumneavoastră.

Comercianților care acceptă tranzacțiile CNP li se solicită să le efectueze în conformitate cu standardele PCI DSS și să respecte în continuare acest standard, și anume, din cauza riscului crescut al prejudiciilor, furtului sau folosirea abuzivă a datelor în mediul CNP.

Mai multe informații privind PCI DSS le găsiți la pag. 513, eventual puteți accesa site-ul www.pcisecuritystandards.org, unde aveți la dispoziție ultima versiune a standardului PCI DSS și instrucțiunea despre modul în care trebuie să asigurați conformitatea cu acest standard

Procesarea tranzacțiilor terților

Prelucrarea tranzacțiilor în folosul altei companii poate să vă provoace prejudicii financiare substanțiale. Fie că vi se oferă plata paușal pentru care acordați un acces nelimitat și utilizarea dispozitivului Dumneavoastră pentru prelucrarea plăților cu cardul, sau comisionul din fiecare plată pe care o procesați, rețineți că doar rareori se întâmplă ca acest terț să acorde în realitate serviciile promise. Aceste entități, deși par să fie entități oneste și invocă motive aparent credibile, din ce cauză au nevoie de asistența Dumneavoastră, sunt doar tertipuri utilizate de bandele de crimă organizată care comit fraude, spre exemplu, legate de vânzarea de locuințe sau bilete.

Să nu acceptați **niciodată** asemenea tranzacții. Tranzacțiile de acest fel sunt în majoritate atacate din partea clientului sau este vorba despre tranzacțiile frauduloase și pot avea drept consecință chargeback-ul sau pierderea financiară pentru activitatea Dumneavoastră comercială. Dacă apare o asemenea situație veți răspunde pe deplin de compensarea financiară a titularului de card, căruia nu i-au fost livrate bunurile achiziționate și serviciul.

Procesarea tranzacțiilor terților prejudiciază de asemenea Contractul nostru privind procesarea tranzacțiilor de plată cu cardul și demascarea acestui tip de activitate poate să aibă drept consecință încetarea imediată a raportului nostru contractual și acceptarea cardurilor de plată. Tipul menționat mai sus de procesare a tranzacțiilor poate duce, de asemenea, la urmărirea penală.

Terminalele

Răspundeți de dispozitivul terminalului și de aceea vă recomandăm cu fermitate să acordați atenția cuvenită locului și verificării periodice a acestui dispozitiv. Răspundeți de asemenea pentru toate pierderile care vor fi produse prin intervenția terților care nu sunt autorizați să manipuleze dispozitivul în alt mod decât cel de efectuare obișnuită a tranzacției, adică, spre exemplu, introducerea PIN-ului.

Asigurați-vă că niciun dispozitiv de securitate (spre exemplu, camera de supraveghere) nu poate să facă înregistrarea titularului de card atunci când se introduce PIN-ul.

TRANZACȚIILE ÎN CARE CARDUL ESTE PREZENT (CP)

Tranzacțiile „cardul prezent“ (CP) sunt orice fel de tranzacții unde cardul și titularul de card sunt fizic prezenți împreună cu Dumneavoastră pe tot parcursul tranzacției și unde vă puteți convinge de prezența cardului de pe care este introdusă tranzacția în terminalul electronic.

Tranzacțiile CP pot fi acceptate și verificate printr-o serie de metode:

- cu CIP-ul și PIN-ul
- cu CIP-ul și prin semnătură
- Contactless
- Cu banda magnetică și PIN-ul
- Cu bandă magnetică și prin semnătură
- Prin introducere manuală (dacă aveți permisă această funcție).

Pe terminalul Dumneavoastră vor apărea instrucțiunile care vă spun cum trebuie să procedați. Informațiile detaliate privind folosirea terminalului Dumneavoastră de plată le găsiți în Manualul utilizatorului de la terminalul Dumneavoastră de plată care este la dispoziție pentru descărcare pe Portalul Comerciantului.

VERIFICAREA TITULARULUI DE CARD CU AJUTORUL PIN-ULUI

În funcție de tipul terminalului, fie Dumneavoastră, fie titularul de card, introduceți cardul în cititorul de carduri al terminalului sau PIN pad-ul extern.

Cerința de a efectua controlul fizic sau vizual al cardului depinde dacă, oricând, pe parcursul tranzacției, manipulați realmente cardul. Dacă manipulați cardul, atunci trebuie să procedați așa cum este menționat în capitolul „Verificarea cardurilor“ de la pagina 13. Nu este necesar să obțineți semnătura clientului pe chitanță sau documentul tipărit de terminal.

VERIFICAREA TITULARULUI DE CARD PRIN SEMNĂTURĂ

Există anumite împrejurări în care identitatea titularului de card nu poate fi verificată prin intermediul PIN-ului. Aceste împrejurări includ:

- cardul fără CIP (spre exemplu, cardul cu bandă magnetică)
- cardul cu CIP care nu folosește ca metodă, verificarea PIN-ului.

În aceste situații, titularul de card nu va fi solicitat să introducă PIN-ul și în loc de aceasta trebuie să se facă verificarea titularului de card prin semnătura lui. Ținând cont de faptul că veți manipula cardul, din partea Dumneavoastră se va solicita efectuarea controlului fizic și vizual, așa cum este descris în capitolul „Verificarea cardurilor“ de la pagina 13.

VERIFICAREA TITULARULUI DE CARD PRIN INTERMEDIUL PIN-ului ȘI AL SEMNĂTURII

Există anumite tipuri de carduri care, chiar dacă este vorba de cardul cu bandă magnetică care solicită verificarea prin semnătură, pot solicita de asemenea și verificarea PIN-ului. Spre exemplu, cardurile UnionPay sunt carduri cu bandă magnetică, în majoritatea situațiilor solicită de asemenea introducerea online a PIN-ului din șase cifre și semnătura.

PLĂȚILE CU CARDUL CONTACTLESS

Plățile cu cardul contactless permit efectuarea tranzacțiilor cu o sumă mică, fără a fi necesar să fie introdus cardul în cititor sau să treacă prin cititorul benzii magnetice.Pentru procesarea acestor plăți este solicitat cititorul contactless care este integrat în terminalul Dumneavoastră de plată. În card este introdusă o tehnologie specială care îi dă posibilitatea să funcționeze în mediul contactless.

Cardurile obișnuite cu bandă magnetică sau cardurile cu CIP nu vor funcționa prin introducerea PIN-ului cu cititorul contactless. În general acest lucru este valabil dacă pe partea frontală sau dorsală a cardului este reprezentat următorul simbol, iar cardul folosește tehnologia contactless (fără contact).

Cu toate că pentru efectuarea plății contactless a cărei valoare este sub limita pentru plățile contactless, aceasta însemnând că este vorba despre o tranzacție de până la 100 RON nu este solicitat PIN-ul, uneori se poate întâmpla ca terminalul Dumneavoastră va solicita efectuarea tranzacției prin introducerea PIN-ului, în locul tranzacției contactless. Este vorba de o funcție suplimentară de securitate al cărei scop este de a confirma că titularul de card posedă realmente cardul – în asemenea situație trebuie să procedați în continuare ca și la tranzacția cu citirea CIP-ului și prin introducerea PIN-ului.

Tehnologia contactless poate fi de asemenea integrată în alte dispozitive, spre exemplu în ceasurile inteligente, brățările, telefoanele inteligente, tabletele și brelocurile electronice pentru chei.

VERIFICAREA CARDURILOR

Tipul de card stabilește ce verificări sunt necesare.

Cum se face verificarea cardului de plată

Există o serie de diferite tipuri de carduri de credit și de debit. Descrierea elementelor de verificare menționate mai jos se referă la majoritatea cardurilor emise de bănci sau de alte instituții financiare. În cazul în care nu veți face aceste verificări, împotriva dumneavoastră poate fi aplicat chargeback-ul:

1. CIP-ul
- Dacă CIP-ul este pe card, verificați, dacă nu poartă semne de încercare de a fi înlăturat, schimbat sau distrus.

2. Numărul cardului
- Numărul de cont al titularului de card începe cu cifra 2 sau 5 pentru cardurile Mastercard, 6 pentru Maestro, 4 pentru Visa, 36 pentru Diners Club, 6011, 64 sau 65 pentru Discover, 62 pentru UnionPay[1], 35 pentru JCB și 37 pentru cardurile Amex.

- Primele patru cifre ale numărului de cont se pot repeta deasupra sau sub începutul numărului în relief al cardului – verificați dacă sunt identice cu primele patru cifre ale numărului în relief, dacă acestea sunt introduse pe card.

- Ultimele patru cifre ale numărului cardului de pe partea frontală a cardului trebuie să fie identice cu numărul de pe spatele cardului de pe banda pe care se semnează (în cazul în care este introdus pe card) și de asemenea cu ultimele patru cifre ale numărului cardului de pe chitanța tipărită de terminal.

- La cardurile în relief (embosate), verificați numerele. Dacă zona din jurul lor este distrusă, aceasta poate să însemne că numerele inițiale au putut fi înlăturate și înlocuite cu altele noi.

- Numărul de card de pe partea frontală a cardului ar fi putut fi tipărit și nicidecum înlăturat și de aceea contactul poate să fie mai degrabă fin decât un contact ieșind în relief.

3. Formula de adresare și numele titularului de card
- Verificați, dacă între titularul de card și datele de pe card nu sunt evidente neconcordanțe, cum este cazul, spre exemplu, dacă o femeie folosește cardul pe care este trecută formula de adresare „Mr.“ sau dacă adolescentul folosește cardul cu titlul de „Doctor“.

- Unele carduri conțin fotografia titularului. Este necesar să verificați dacă fotografia corespunde persoanei care prezintă cardul și dacă fotografia nu a fost schimbată.

4. Valabil de la/expirarea valabilității/valabil până la
- Este necesar să examinați cu atenție privitor la valabilitatea cardului. Nu acceptați cardurile care sunt prezentate pentru efectuarea tranzacției înaintea datei „valabil de la“ (unde este trecută această dată) sau după data expirării valabilității “valabil până la”. Terminalul face automat anumite controale pe card, cu toate acestea nu poate să ne facă responsabili pentru faptul că terminalul acceptă un card care nu mai este valabil sau un card cu valabilitatea expirată.

5. Hologramа
- Verificați să nu prezinte semne de manipulare. Hologramа ar trebui să fie fină la atingere și nu ar trebui să aibă suprafața grosieră sau zgâriată, iar imaginea 3D ar trebui să se miște prin înclinare.

[1] Cardurile UnionPay cu două semne încep de asemenea cu cifra 3, 4, 5 sau 9

Cardurile contrafăcute conțin deseori imitații piratate ale hologramelor.

- Holograma este dispusă pe partea frontală sau dorsală a cardului, cu excepția cazului când pe card este utilizată banda Holomag (banda magnetică holografică) în locul benzii magnetice tradiționale.

- Printre cele mai frecvente forme de holograme se numără:
  – Mastercard – imaginea globului pământesc
  – Visa – o porumbiță în zbor sau câteva porumbițe în zbor
  – Visa Electron – nu toate cardurile conțin o hologramă. Dacă apare holograma pe card, aceasta arată ca o porumbiță în zbor
  – UnionPay- imaginea 3D a Templului ceresc
  – Diners – un cerc împărțit
  – JCB – zorii zilei
  – Amex – centurionul roman

6. Banda pe care se semnează

- Rețineți – dacă cardul este verificat cu ajutorul PIN-ului, nu este necesar să se verifice dacă semnătura corespunde.

- Semnătura ar trebui să fie scrisă clar și ar trebui să fie netedă la atingere. Să fiți suspicioși, dacă se pare că semnătura a fost ștearsă, dacă se pare că pe card este transcrisă semnătura sau dacă semnătura a fost scrisă cu litere majuscule sau a fost scrisă cu markerul.

- Verificați dacă semnătura corespunde numelui introdus pe partea frontală a cardului.

- Verificați dacă banda pe care se semnează nu are semne de manipulare sau dacă pe ea nu se văd resturi în urma semnăturii șterse.

- Verificați dacă semnătura de pe card corespunde semnăturii de pe chitanța tipărită de terminal.

Dacă vă este prezentat un card nesemnat, solicitați-i titularului de card să facă dovada identității sale și să semneze cardul în prezența Dumneavoastră. Notați tipul și numărul actului de identitate pe documentul de vânzare și autorizați tranzacția fără a ține cont de valoarea limitei de tranzacționare.

7. Codul de siguranță al cardului (CSC)/Cifrele de control (CVV2)

- Codul de verificare din trei sau patru cifre. La cardurile Mastercard, Visa și Maestro codul CSC reprezintă ultimele cifre tipărite pe partea dorsală a cardului, după ultimele patru cifre ale numărului de cont al titularului de card, dacă acestea sunt introduse acolo. Codul CSC poate fi de asemenea introdus pe însăși banda pe care se semnează sau în caseta albă din dreapta, față de banda pe care se semnează. La cardurile American Express acest număr are patru cifre și este tipărit pe partea frontală a cardului.

8. Banda magnetică

- Asigurați-vă că respectivul card are banda magnetică pe partea dorsală. Dacă banda magnetică la atingere esteneobișnuit de grosieră sau zgâriată, trebuie să se ia în considerare suspiciunea că respectivul card a fost contrafăcut.

- Unele carduri au banda Holomag (banda magnetică holografică) în locul benzii magnetice tradiționale. Dacă pe card este prezentă banda Holomag, aceasta trebuie să fie întotdeauna pe partea dorsală a cardului și cardul nu mai trebuie să conțină nicio altă hologramă.

9. Elementele ultraviolete

- Dacă aveți un tester UV pentru bancnote, puteți efectua controlul semnului ultraviolet pe partea frontală a cardurilor.

10. Fotografiile

- Unele carduri conțin fotografia titularului de card, și anume, în dreapta, pe partea frontală a cardului. Dacă Vă este prezentat un card care conține acest element, verificați dacă fotografia corespunde persoanei care prezintă cardul pentru efectuarea tranzacției. În cazul în care între fotografie și titular nu este o conformitate, este justificat să se considere suspiciune.

11. Siglele de pe carduri

- Siglele de pe carduri – se află de regulă pe partea frontală a cardului, cu toate acestea pot apărea și pe partea dorsală. Ar trebui să iasă clar în evidență și să fie în culori stridente – sigla (logotipul) care este ștearsă în jurul marginilor sau care iese în evidență prin calitatea proastă, poate să indice faptul că respectivul card a fost contrafăcut.

Dacă aveți orice suspiciune privind cardul sau titularul ei, contactați la telefon centrul de asistență și comunicați-i „codul 10". (consultați pagina 52).

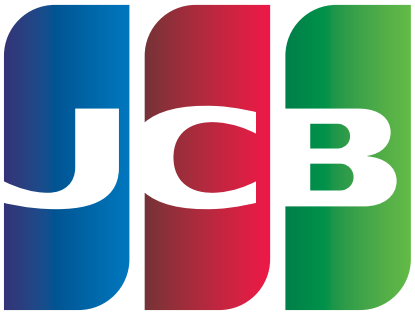
EXEMPLE DE SIGLE PE CARDURI

Mastercard

Discover

Visa

UnionPay



JCB

EXEMPLE DE CARDURI ȘI ELEMENTELE DE PE CARDURI

Legenda pentru imaginile cardurilor:

1. CIP-ul
2. Numărul cardului
3. Titlul și numele titularului de card
4. Valabil de la/data expirării valabilității (legenda „Valid Thru" introduce ultima lună de valabilitate)
5. Sigla contactless (dacă este inclusă pe card)
6. Sigla (logotipul) cardului
7. Holograma
8. Banda pe care se semnează
9. Codul de siguranță al cardului (CSC)
10. Banda magnetică/banda Holomag
11. Alte semne pentru acceptarea cardului

Mastercard

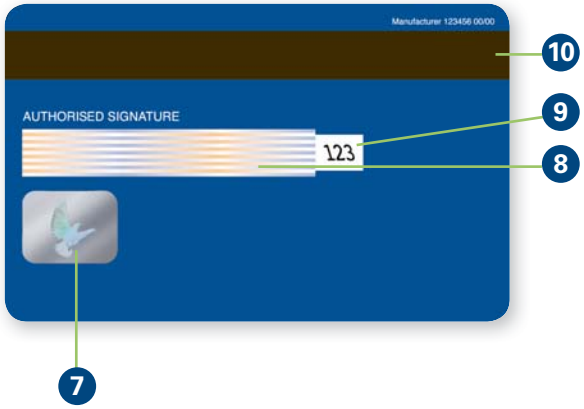
Fata

Verso

Visa

Fata

Verso



UnionPay

Fata

Verso

JCB (Japan Credit Bureau)

Fata

Verso

ACCEPTAREA CARDURILOR PRIN INTERMEDIUL TERMINALULUI DE PLATĂ (POS)

Puteți accepta cardurile fie prin intermediul terminalului furnizat de noi, sau, de comun acord în prealabil, cu ajutorul propriului Dumneavoastră dispozitiv.

Utilizarea terminalului furnizat de noi

Înainte de a începe:

- Citiți instrucțiunea de folosire a terminalului, întrucât găsiți acolo informațiile privind acceptarea cardurilor.
- Verificați dacă data și ora sunt corecte la terminalul Dumneavoastră. Dacă nu sunt corecte, efectuați resetarea lor pe baza indicațiilor din instrucțiunea de utilizare a terminalului.
- În cazul amplasării terminalului sau a PIN pad-ului, țineți cont de accesibilitatea tuturor titularilor de carduri, inclusiv a celor cu handicap.
- Asigurați-vă că veți avea acces facil la prizele electrice și de telefon de la terminalul Dumneavoastră cu card, în cazul în care apar orice probleme tehnice și vom solicita din partea Dumneavoastră să faceți anumite teste în cadrul identificării problemei.
- Asigurați-vă că niciun dispozitiv de securitate (spre exemplu, camerele de supraveghere) nu poate să-l înregistreze pe clientul care introduce PIN-ul

Vă rugăm să vă consultați cu noi pentru orice schimbări care apar la terminalul Dumneavoastră, inclusiv schimbările lui, eliminarea sau transferarea. În cazul terminalelor mobile este permisă transferarea zilnică în cadrul utilizării lor curente.

În cazul în care aveți nevoie de orice asistență, vă rugăm să ne sunați (consultați pag. 52, unde sunt menționate datele noastre de contact).

Utilizarea propriului dispozitiv

Serviciile de procesare a tranzacțiilor le acordăm de asemenea companiilor care acceptă cardurile de plată cu ajutorul propriului dispozitiv sau al sistemului de acceptare a cardurilor (inclusiv orice piese din acest dispozitiv oferite de terț).

Avem capacitatea de a sprijini ambele sisteme principale de acceptare a cardurilor de plată care sunt:

- sistemele caselor de marcat (EPOS), având capacitatea de a accepta cardurile
- terminalele electronice pentru acceptarea cardurilor de plată care funcționează independent de casa de marcat.

Pentru ambele sisteme vă putem oferi:

- specificațiile de sistem care includ amănunțit cerințele noastre și interfața.

Trebuie să testăm și să omologăm toate dispozitivele înainte de implementare. În cazul în care utilizați propriile Dumneavoastră dispozitive trebuie să vă conduceți după procedurile descrise în această instrucțiune, chiar dacă nu cădem de acord asupra procedurilor alternative și/sau suplimentare pe care le vom documenta separat.

Este necesar să ne informați asupra tuturor modificărilor propuse referitoare la terminale, reglarea lor și legăturile de transfer. Dacă nu veți proceda în acest fel, se poate întâmpla să nu putem procesa tranzacțiile Dumneavoastră și să apară întârzieri în creditarea acestor tranzacții în contul Dumneavoastră bancar.

Dacă îi folosiți pe terți în calitate de prestatori, trebuie să ne informați despre orice schimbare a acestui prestator. Trebuie de asemenea să vă asigurați că prestatorul respectă standardele Payment Card Industry Data Security Standard (PCI DSS, vezi pag. 41)

Răspunderea Dumneavoastră este să vă asigurați că dispozitivul Dumneavoastră pentru acceptarea cardurilor de plată îndeplinește standardele de securitate obișnuite pentru domeniul respectiv. Trebuie să efectuați și să achitați cheltuielile pentru toate upgrade-urile dispozitivului Dumneavoastră pe care putem să îl solicităm noi sau furnizorul terminalului Dumneavoastră, în caz de necesitate. Cele menționate mai sus cuprind toate îmbunătățirile care trebuie efectuate, pentru ca dispozitivul Dumneavoastră să corespundă schimbărilor din regulamentul operatorului. Incapacitatea de a reacționa la aceste schimbări poate produce un dezacord cu dispozițiile menționate mai sus și poate avea drept consecință comisioane și amenzi și un risc sporit de chargeback-uri.

AUTORIZAREA

Autorizarea proceselor tranzacționale se definește prin identificarea distinctă a tuturor jucătorilor implicați în cadrul procesului, astfel fiind necesară identificarea cu exactitate a procesatorului, acceptatorului și a emitentului titlului de plată. În funcție de modul de autorizare există mai multe tipuri de procese de autorizare.

Autorizarea Online

Pentru autorizarea Online, tranzacția este expediată imediat la centrul de autorizare. Suma autorizată se citește în sumele terminalelor pentru scopuri de control și administrative. Astfel sunt procesate toate tranzacțiile cu cardurile bancare, cu excepția tranzacțiilor descrise în secțiunea de autorizare Offline.

Autorizarea Offline

Pentru autorizarea Offline, tranzacția este autorizată în terminal. Astfel sunt autorizate tranzacțiile efectuate cu cardurile contactless și cu contact ale căror valoare și număr sunt evaluate individual și aprobate de procesator.

Autorizarea Semi-Offline

Pentru autorizarea Semi-offline, tranzacția este autorizată în terminal și după terminarea tranzacției este expediată în contextul tipăririi chitanțelor la centrul de autorizare pentru procesarea ulterioară.

Dacă tranzacția a fost acceptată, în conformitate cu setarea terminalului, datele, fie se expediază imediat, fie se introduc în terminal și trebuie să fie trimise în cadrul lotului, la centrul de autorizare.

Autorizarea la terminalul POS este asigurată automat, dacă suma de vânzare depășește limita de autorizare.

Autorizarea nu efectuează confirmarea identității titularului de card și nici nu constituie garanția plății.

Dacă aveți orice suspiciune privind cardul sau titularul acestuia, contactați telefonic centrul de asistență și comunicați-i „codul 10“ (vezi pagina 52).

Pre-autorizarea

Pre-autorizarea se folosește în cea mai mare parte în domeniul turismului, îndeosebi în unitățile de cazare și la firmele de închirieri, unde suma finală a tranzacției nu este cunoscută în momentul autorizării inițiale. Pre-autorizarea reprezintă procesul prin care se efectuează verificarea valabilității cardului de plată la comerciant și a disponibilității fondurilor în contul titularului cardului de plată pentru tranzacția de plată presupusă.

Pre-autorizarea se poate efectua doar prin intermediul terminalului electronic de plată POS pentru toate tipurile de carduri, cu excepția cardului de plată Maestro, Mastercard Electronic, Visa Electron și V PAY. Comerciantul este obligat să încheie pre-autorizarea în cel mult 30 de zile de la data începerii pre-autorizării.

Suma de pre-autorizare trebuie să corespundă întotdeauna prețului prealabil al serviciului sau bunurilor convenit între comerciant și titularul de card. Titularul de card trebuie să fie informat dinainte referitor la pre-autorizare și trebuie să fie de acord cu aceasta.

Procedurile cum trebuie să se realizeze tranzacția de ‚Pre-autorizare', sunt descrise în Manualul utilizatorului pentru terminalul de plată.

Terminarea pre-autorizării

Tranzacția de terminare a pre-autorizării reprezintă practic definitivarea vânzării care a fost mai întâi pre-autorizată. Suma de terminare a pre-autorizării poate să fie diferită de suma introdusă pentru pre-autorizare. Terminarea pre-autorizării poate fi de asemenea efectuată și în lipsa titularului de card. Acest tip de tranzacție se poate efectua prin utilizarea CIP-urilor magnetice și de asemenea a cardurilor contactless.

În momentul în care doriți să încheiați pre-autorizarea, trebuie să aveți pregătit codul de autorizare cu 6 cifre și identificatorul din 9 cifre de pe chitanța de pre-autorizare. De asemenea trebuie știți suma reală pentru terminarea pre-autorizării.

Pentru terminarea pre-autorizării la terminalul Dumneavoastră de plată procedați exact conform instrucțiunilor menționate în Manualul utilizatorului.

Stornarea tranzacției arbitrare

Tranzacția de stornare servește pentru anularea oricărei tranzacții a cărei vechime nu a depășit 95 de zile. Tranzacția se poate storna la orice terminal în cadrul unui loc de tranzacționare (al unității). Suma se poate storna la valoarea totală a tranzacției, sau doar parțial. Dacă la tranzacția stornată s-au folosit serviciile DCC, este posibil să se anuleze doar întreaga tranzacție și suma pentru stornare este introdusă în RON.
Procedura detaliată de stornare a tranzacției este descrisă în Manualul utilizatorului pentru Terminalul Dumneavoastră de plată.

Ce fel de raport va apărea pe terminalul meu?

În momentul când a fost generată automat cererea de autorizare, terminalul afișează mesajul de raspuns. Pot apărea următoarele tipuri de mesaje:

ACCEPTAT
Autorizarea s-a efectuat cu succes. Tranzacția este acceptată.

ACCEPTAT – VERIFICAȚI IDENTITATEA
„autorul- codul xxxxxx"
Tranzacția este acceptată și identitatea titularului de card trebuie să fie verificată. Scrieți pe chitanță numărul și tipul documentului de identitate.

„SUNAȚI LA AC", „SUNAȚI LA- CENTRUL DE AUTORIZARE VOCALĂ/"
Dacă pe terminalul Dumneavoastră apare unul din aceste mesaje în momentul când încercați să obțineți autorizarea automată, trebuie să sunați la centrul nostru de asistență (datele de contact le găsiți la pag. 52). Aceste rapoarte înseamnă că trebuie să efectuăm verificările suplimentare de securitate care sunt solicitate de emitentul cardului. Întotdeauna trebuie să sunați la centrul nostru de asistență înainte de a accepta altă modalitate de plată.

„REFUZAT"
Tranzacția nu se poate efectua. Dacă împreună cu titularul de card doriți să continuați vânzarea, solicitați-i o modalitate alternativă de plată.

„CARD NEAUTORIZAT"
Verificați dacă aveți autorizarea de acceptare a acestui tip de carduri. Dacă nu sunteți siguri, ar trebui să contactați centrul de asistență (datele de contact le găsiți la pag.52). Dacă aveți autorizarea de acceptare a cardului de tipul prezentat, vă rugăm să sunați la centrul nostru de asistență și să îi comunicați „codul 10" (vezi pagina 52).

„CARD NEACCEPTAT"
Cardul nu se poate folosi pentru tipul de tranzacție. Puteți solicita altă modalitate alternativă de plată.

„REȚINEȚI CARDUL"
Indicația de a reține cardul cu care este efectuată tranzacția a fost initiat de banca emitenta.

„CARD NEVALABIL"
Perioada de valabilitate a cardului s-a încheiat sau a fost introdus eronat numărul cardului prin introducerea manuală sau sunt informații eronate în înregistrarea magnetică. Tranzacția nu se poate efectua.

„TIMPUL A EXPIRAT"
La procesarea tranzacției s-a produs o eroare și sistemul nu a returnat răspunsul la cerința de autorizare în limita de timp.

Dacă terminalul Dumneavoastră nu este setat pentru a efectua automat autorizarea, sau dacă pe acesta apare o eroare care împiedică terminalul Dumneavoastră să obțină automat autorizarea, este necesar să sunați la centrul nostru de asistență (datele de contact le găsiți la pag. 52).

Limitele de autorizare

Limitele de autorizare sunt setate de emitentul cardurilor de credit. Emitentul poate totuși să seteze limita de autorizare preferată de el de pe card, care poate să aibă apoi prioritate față de limita setată la terminal.

În caz de necesitate, putem schimba limita Dumneavoastră de autorizare în cadrul tendinței noastre de luptă împotriva fraudelor sau la cererea emitentului cardurilor de credit. Referitor la orice eventuală schimbare vă vom informa și vă oferim instrucțiunile necesare.

APELUL TELEFONIC CUPRINZÂND COMUNICAREA „CODULUI 10"

Convorbirea telefonică cuprinzând comunicarea „codului 10" ar trebui să fie efectuată prin a suna la centrul nostru

de asistență (datele de contact sunt menționate la pag. 52), dacă:

- aveți orice suspiciune referitoare la card, titularul de card, sau împrejurările tranzacției
- ați primit de la noi indicația de a acționa astfel, ca o măsură de prevenire a fraudelor.

Ce vă trebuie pentru apelul telefonic care conține comunicarea „Codului 10“

- numărul comerciantului
- valoarea tranzacției, rotunjită în RON; dacă tranzacția nu este efectuată în RON, introduceți valuta și suma
- codul de autorizare, dacă respectivul cod a fost oferit cu tranzacția inițială, spre exemplu, împreună cu autorizarea online
- va fi necesar să menționați clar de ce aveți suspiciunea referitoare la card și/sau titularul acestuia
- ar trebui să vă asigurați că efectuați convorbirea cât mai discret
- puteți primi indicația de a-i adresa titularului de card o serie de întrebări din motive de securitate.

Aceste controale de siguranță le-ați putea efectua și atunci, când clientul vă oferă o modalitate alternativă de plată. Este important să efectuați convorbirea telefonică cuprinzând comunicarea „codului 10“ și atunci când clientul Dumneavoastră solicită returnarea cardului sau dacă părăsește spațiile, fără ca tranzacția să fi fost încheiată.

NU UITAȚI SĂ:

- îl atenționați pe titularul de card asupra faptului că imediat va fi efectuat controlul de siguranță sau că procesatorul Dumneavoastră de carduri a solicitat verificarea de siguranță de rutină a tranzacției. Pastrati cardul și bunurile la Dumneavoastră, până când nu se fac controalele de siguranță.
- sunați la centrul nostru de asistență (datele de contact sunt menționate la pag. 52).
- obțineți codul de autorizare direct de la noi și nicidecum de la titularul de card sau de la oricine altul, cum este, spre exemplu, emitentul cardului care ar putea fi cuplat la convorbire
- nu sunați la niciun număr de telefon pe care vi-l dă titularul de card
- nu efectuați apelul telefonic cuprinzând comunicarea „codului 10“, dacă vă simțiți amenințați sau considerați că nu este sigur, spre exemplu, dacă sunteți singuri în magazin; în acest caz, sunați-ne imediat ce a plecat titularul de card, întrucât un asemenea apel telefonic poate să ajute la împiedicarea altor activități frauduloase comise în altă parte.

La reținerea cardului nu ar trebui să vă expuneți pericolului nici pe Dumneavoastră înșivă și nici pe colegii Dumneavoastră. Dacă persoana care prezintă cardul pentru tranzacție începe să se comporte agresiv sau violent, să-i restituiți întotdeauna cardul, și anume, chiar și atunci când v-am solicitat reținerea acestuia.

Dacă există permanent suspiciunea

După ce ați efectuat convorbirea cuprinzând comunicarea „codului 10“ și ați obținut autorizarea, nu sunteți în niciun fel obligați să încheiați tranzacția.

Însă, în asemenea caz, nu trebuie să rețineți cardul.

CARDURILE REȚINUTE

Reținerea cardului

Dacă vă solicităm să rețineți cardul, încercați, vă rugăm, să faceți acest lucru.

Dacă persoana care prezintă cardul pentru tranzacție începe să se comporte agresiv sau violent, să-i restituiți întotdeauna cardul, și anume, chiar și atunci când v-am solicitat reținerea cardului. În această situație ar trebui ca întotdeauna:

- să încercați să înregistrați detaliile privind aspectul persoanei care prezintă cardul pentru tranzacție și să folosiți dispozitivul de monitorizare (spre exemplu, camera de supraveghere), dacă o aveți la dispoziție
- să sunați la centrul nostru de asistență (datele de contact sunt menționate la pag. 52) și să ne explicați

că nu ați putut să rețineți cardul, așa cum ați fost solicitați.

În anumite împrejurări vom contacta poliția. Dacă poliția solicită cardul:
- transmiteți cardul poliției

- înregistrați numele polițistului, numărul lui de identificare și numărul de telefon al secției de poliție

- aduceți-i la cunoștință polițistului anchetator, dacă ați folosit camera de supraveghere, iar eventuala înregistrare video cu materialul probatoriu să o păstrați timp de cel puțin 30 de zile.

Dacă se reține cardul:
- completați imediat Formularul privind reținerea cardului

- oferiți cât mai multe informații despre persoana care a prezentat cardul pentru tranzacție și alte informații relevante, cum este, spre exemplu, numărul de înmatriculare al vehiculului acesteia

- tăiați cardul în jumătate, longitudinal, pentru ca banda pe care se semnează, banda magnetică, numărul cardului în relief, hologrma și CIP-ul să rămână nedistruse

- transmiteți-ne imediat ambele părți ale cardului și Formularul completat privind reținerea cardului, la adresa sdiului central.

- păstrați-vă o copie după Formularul de reținere a cardului.

Sediul central (adresa la care trebuie să trimiteți cele menționate mai sus):
Global Payments s.r.o.
Str. V Olšinách Nr . 626/80
Codul poștal 100 00, Praga 10 – Strašnice
Republica Cehă

Sucursala locala:
Praga Sucursala București
Calea Victoriei, nr. 15
Sector 3,
România

Găsirea cardului sau cardul uitat în spațiile unității Dumneavoastră

Vă rugăm să păstrați toate cardurile uitate ale clienților, într-un loc sigur (spre exemplu, seiful, conform standardelor PCI DSS), timp de 24 ore.

Dacă se prezintă clientul pentru card, nu-i transmiteți cardul până nu ați verificat identitatea titularului de card:
- solicitați-i un act de identitate, cum este, spre exemplu, permisul de conducere

- verificați semnătura de pe card față de specimenul de semnătură al persoanei care s-a prezentat pentru card

- dacă aveți îndoieli, contactați centrul nostru de asistență (datele de contact sunt menționate la pag. 52).

Dacă nu se prezintă nimeni pentru card în cel mult 24 de ore:
- tăiați cardul în jumătate, longitudinal, pentru ca banda pe care se semnează, banda magnetică, numărul cardului în relief și CIP-ul să rămână nedistruse

- Completați formularul privind reținerea cardului

- Transmiteți-ne ambele părți ale cardului, împreună cu Formularul privind reținerea cardului la adresa sediului central.

RAMBURSAREA BANILOR

Banii pot fi rambursați doar cu același card care a fost folosit la tranzacția inițială de vânzare.
- Suma rambursată nu trebuie să depășească suma tranzacției inițiale.

- Să nu rambursați niciodată banii în alt mod și să nu dați posibilitatea de rambursare a banilor în numerar sau prin transfer în contul bancar ș.a.m.d.

Anularea tranzacției

Dacă titularul de card decide să nu cumpere bunurile sau serviciile, trebuie să anulați tranzacția. Pașii pe care trebuie să-i urmați sunt în funcție de cum ați primit cardul și de faza în care se afla tranzacția, în momentul în care titularul de card s-a decis s-o anuleze.

Dacă nu ați terminat tranzacția:

- Cu PIN-ul verificat – puteți anula tranzacția când introduceți suma folosind tastatura terminalului. Eventual, titularul de card poate să anuleze tranzacția prin introducerea PIN-ului.

- Prin verificarea semnăturii – puteți anula tranzacția în momentul în care terminalul Dumneavoastră vă cere confirmarea semnăturii titularului de card.

- Anularea oricărei tranzacții încheiate după mai mult de 95 de zile – vezi manualul utilizatorului pentru terminalul Dumneavoastră.

Imediat ce anularea este efectuată, ar trebui să-i oferiți titularului de card o copie după documentul care confirmă anularea.

Procesarea tranzacțiilor

Oferim decontarea care se desfășoară 7 zile pe săptămână. Termenul de sistem pentru închidere de zi este 22:55. Toate tranzacțiile prezentate spre decontare înainte de acest termen vor fi trimise din contul nostru în contul Dumneavoastră în ziua următoare, deci, D[2] +1. Toate tranzacțiile efectuate după acest termen de sistem vor fi trimise din contul nostru, în cea de a 2-a zi care se succede, deci, D+2.

[2] D… ziua efectuării tranzacției

TRANZACȚIILE ÎN CARE CARDUL NU ESTE PREZENT (CNP)

Tranzacțiile în care cardul nu este prezent (CNP) sunt orice fel de tranzacții în care cardul și titularul de card lipsesc fizic, în momentul tranzacției.

Aceste tranzacții reprezintă o ocazie pentru fraude, întrucât cardul, semnătura și numărul personal de identificare (PIN-ul) nu se pot verifica.

MO/TO - PRIMIREA COMENZILOR TELEFONICE ȘI A COMENZILOR PRIN POȘTĂ

MO/TO este tranzacția efectuată pe baza comenzii în scris sau telefonice pentru bunuri sau servicii și a acordului titularului de card. Plata este efectuată ulterior fără prezentarea fizică a cardului acestuia, de către titular față de prestatorul de bunuri sau servicii, adică față de comerciant.

Tranzacțiile MO/TO se pot efectua doar la terminalul de plată și doar dacă aveți încheiat cu noi un contract de acceptare a acestui tip de tranzacții, în scris.

Dacă acceptați tranzacțiile MO/TO, trebuie să vă asigurați că titularul de card vă oferă următoarele informații:

- tipul de card
- codul de siguranță al cardului (CSV)
- numărul cardului
- numele și inițialele, exact așa cum sunt introduse pe card
- data începerii valabilității (dacă este introdusă pe card)
- data expirării
- numele de pe extrasul de card
- adresa de pe extrasul de card
- numărul de telefon de contact (vă recomandăm să nu acceptați numărul de telefon mobil).

Pe titularul de card trebuie să îl informați referitor la valoarea totală a tranzacției (inclusiv a valutei) și să obțineți de la acesta acordul lui în scris pentru a retrage această sumă de pe cardul lui.

Trebuie, de asemenea, să vă asigurați că:

- toate comenzile în scris cuprind semnătura titularului de card
- introduceți procesul cu ajutorul căruia veți verifica dacă diferitele tranzacții se referă la una și aceeași adresă sau dacă același număr de card este folosit pentru diferite adrese

La anularea comenzii efectuați rambursarea întotdeauna doar cu cardul de plată care a fost folosit pentru efectuarea tranzacției inițiale. Nu rambursați niciodată banii în alt mod.

Efectuarea tranzacției MO/TO la terminalul Dumneavoastră de plată

Tranzacția se poate efectua doar prin introducerea manuală a numărului de card. Acest tip de tranzacție este întotdeauna trimisă spre autorizarea Online. Comerciantul își selectează funcția MENU – Tranzacție – MOTO la terminalul său și apoi continuă, conform instrucțiunilor de la terminalul de plată.

Instrucțiunea detaliată despre modul cum se face acest tip de tranzacție o găsiți în Manualul utilizatorului de la terminalul Dumneavoastră.

GP WEBPAY

GP webpay este un portal de plăți online pentru plățile rapide și în siguranță cu cardul generat de partenerul nostru de service- societatea Global Payments Europe, s.r.o. Acest serviciu dă posibilitatea vânzărilor online de a încasa plățile efectuate cu cardurile de plată Visa, Mastercard și Diners Club. De asemenea, promovează plățile prin intermediul portofelelor digitale MasterPass și Mastercard Mobile. GP webpay promovează în totalitatea standardul 3D Secure.

Principalele avantaje ale portalului GP webpay, pe scurt:

– Încasarea plăților în 3D Secure – cardurile emise de asociațiile Mastercard și Visa

– Încasarea plăților în SSL – cardurile emise de asociația Diners Club și plățile recurente

– Încasarea plăților prin utilizarea portofelului digital – MasterPass și Mastercard Mobile

– Beneficierea, în colaborare cu prestatorul, de funcțiile pentru limitarea fraudelor – Fraud Prevention System

– Beneficierea de interfața API HTTP și API WS (Web Services) pentru integrarea cu eshop

– Beneficierea de portalul GP webpay – administrarea plăților, utilizatorilor și a cheilor, descărcarea documentației tehnice și a celorlalte resurse pentru integrarea cu interfața portalului de plăți GP webpay

– Consultanță și asistență acordate de echipa de specialiști la introducerea și funcționarea acestei soluții

Asigurarea plăților

– GP webpay respectă standardele internaționale și îndeplinește cele mai stricte cerințe de securitate Mastercard SecureCode, Verified by Visa și SafeKey, stabilite de asociațiile de carduri Mastercard și Visa. Aceste standarde sunt marcate cu 3D Secure și asigură securitatea maximă a plății.

– PCI DSS reprezintă un pachet de standarde de securitate al cărui scop este de a limita orice scurgere de informații privind titularii de carduri. Deja de câțiva ani ne supunem controalelor efectuate de un auditor internațional independent care analizează temeinic capacitatea noastră de a proteja datele sensibile.

Dacă doriți să aflați mai multe despre GP Webpay, nu ezitați să ne contactați (datele de contact sunt menționate la pag. 52)

PLATA RECURENTĂ

Funcția de plată recurentă este definită de asociații ca fiind un card cu plata aferentă facturării repetate, având condițiile convenite, stabilite dinainte, de către client, cum sunt, spre exemplu, dată fixă sau suma fixă.

Conștientizarea riscurilor

- Orice plată recurentă procesată după ce titularul de card a anulat autorizarea de plată, va avea drept consecință chargeback-ul.
- Tranzacțiile recurente nu oferă nicio garanție a obținerii definitive a plății și efectuarea acestora este pe propriul risc.
- Dacă titularul de card prezintă o plângere privind tranzacția, nu trebuie să mai procesați alte tranzacții.

Cum trebuie să generați aprobarea în legătură cu acordul privind plata recurentă

Înainte de procesarea primei tranzacții recurente, trebuie să aveți acordul prealabil în scris al titularului de card pentru efectuarea plății recurente. În acest scop, vă recomandăm să vă pregătiți propunerea de Contract privind plata recurentă (Recurring Transaction Agreement, RTA).

RTA trebuie să cuprindă:
- Suma și data
- Dacă suma/data este fixă sau variabilă
- Metoda de comunicare cu clientul

Comerciantul este obligat:
- să confirme contractul RTA clientului în cel mult două zile prin metoda convenită de comunicare
- contractul RTA trebuie să fie păstrat pe durata derulării contractului și oferit la cererea emitentului cardului (pe email sau în alt format electronic, eventual pe suport de hârtie).

De asemenea vă rugăm să vă asigurați că:
- la sumele nespecificate dinainte, titularul de card este informat în scris referitor la valoarea exactă a sumei, cu cel puțin 14 zile înainte ca fiecare sumă să fie contabilizată
- păstrați autorizarea realizată în scris/pe email a titularului de card pe o perioadă de cinci ani de la data ultimei plăți sau de la anularea autorizării (vezi capitolul „Securitatea datelor“ de la pag. 41)
- informați-i pe clienți asupra faptului că aceștia pot oricând să anuleze contractul și informați-i cum vă vor comunica anularea

- la o cerere de anulare veți reacționa rapid
- informațiile de pe card sunt păstrate în siguranță și nu îi includ pe titularii de card CSC.

Cum trebuie să se efectueze tranzacțiile recurente

Prima așa-numita plată de înregistrare se desfășoară ca o plată standard 3D Secure și pentru aceasta trebuie să se facă verificarea titularului cardului de plată și plata. În cazul refuzului plății, prin contractul respectiv RTA nu se pot efectua alte plăți și comerciantul trebuie să îl informeze pe client.

În cazul în care comerciantul oferă gratis o perioadă de probă, clientul trebuie să fie informat cu 7 zile înainte referitor la efectuarea plății la sfârșitul acestei perioade.

Plata recurentă se efectuează prin utilizarea API WS (Web Services), fără redirecționarea browserului clientului pe pagina de plată pentru introducerea informațiilor privind cardul de plată. GP webpay efectuează direct autorizarea plății care se desfășoară prin asigurarea SSL fără verificarea titularului cardului de plată.

Comerciantul ar trebui să îl atenționeze pe client când se apropie sfârșitul valabilității cardului lui și să îi ofere reînnoirea contractului RTA.

Comerciantul trebuie să îl atenționeze pe client cu cel puțin șase zile lucrătoare înainte de următoarea plată recurentă prin metoda convenită de comunicare în toate situațiile următoare:

- De la ultima plată au trecut mai mult de șase luni
- S-a încheiat perioada gratuită de probă, oferta de introducere sau acțiunea de promovare
- În contractul RTA s-a modificat suma și/sau data pentru plata recurentă

Anularea

Comerciantul trebuie să-i faciliteze clientului anularea simplă și ușor disponibilă online a plății recurente.

Plata recurentă poate s-o anuleze, în numele clientului, și emitentul cardului acestuia. În această situație, plata de înregistrare este invalidată și nu se poate genera o plată recurentă pentru aceasta.

Plata de înregistrare este invalidată automat, dacă în decurs de un an nu a fost generată plata recurentă și pentru acesta nu se poate genera plata recurentă.

Specificația tehnică pentru dezvoltatori descrie generarea plății recurente.

Notă importantă: nu este posibil să se efectueze plata recurentă pentru cardurile de plată Maestro.

FASTPAY

Funcția Fastpay dă posibilitatea comerciantului să afișeze clientului înregistrat, pe pagina de plată, ultimele 4 cifre și valabilitatea cardului cu care clientul a achitat plata precedentă. Clientul introduce doar codul de verificare (CVC2/CVV2), plata se efectuează ca și o plată standard 3D Secure, cu verificarea titularului cardului de plată.

Comerciantul ar trebui să-l atenționeze înainte pe client pentru utilizarea acestei funcții.

Clientul poate să transcrie datele afișate și să le plătească cu alt card.

Plata PUSH– primirea comenzilor online

Funcția de plată PUSH dă posibilitatea comerciantului să genereze cerința de plată (așa-numitul link pentru plăți). Comerciantul poate să genereze plata PUSH în portalul GP Webpay așa cum este redat în imaginea de mai jos.

Linkul pentru plăți poate fi trimis ulterior clientului pe email sau poate fi transferat în codul QR. Dacă clientul decide să plătească cu PUSH, dă clic pe linkul pentru plăți, eventual citește codul QR și browserul lui va fi redirecționat spre portalul de plată GP Webpay, unde va achita plata prin același mod ca și în eshop.

PORTALUL GP WEBPAY

Portalul GP webpay îi facilitează utilizatorului comerciantului:

- căutarea și gestionarea plăților
- crearea, trimiterea, căutarea și administrarea plăților PUSH
- crearea și administrarea utilizatorilor
- afișarea statisticii și a funcțiilor autorizate pentru eshop și plăți
- crearea și gestionarea cheilor
- descărcarea documentației tehnice și a celorlalte resurse pentru integrarea cu interfața portalului pentru plăți GP webpay

Informațiile complete privind posibilitățile de utilizare a serviciilor GP Webpay le găsiți în manualele utilizatorului, disponibile online pe adresa www.gpwebpay.cz

TIPURILE SPECIALE DE TRANZACȚII

Această secțiune vă prezintă o serie de tipuri speciale de tranzacții de care puteți avea nevoie, în funcție de metoda prin care oferiți procesarea tranzacțiilor efectuate cu cardul.

CONVERSIA VALUTARĂ DINAMICĂ - DYNAMIC CURRENCY CONVERSION, DCC)

Acest serviciu este deja înregistrat pe terminalul Dumneavoastră de plată (punct de vânzare, point of sale - POS) pe care l-ați primit de la noi, cu toate acestea, pentru activarea lui și pentru a-l oferi clienților este necesar acordul nostru prealabil în scris. Serviciile DCC sunt disponibile pentru tranzacțiile cu cardurile Visa și Mastercard.

O nouă oportunitate pentru activitatea Dumneavoastră comercială

Conversia Valutară Dinamică (DYNAMIC CURRENCY CONVERSION- DCC) oferă o nouă oportunitate de a veni în întâmpinarea posesorilor de carduri internaționale care preferă să plătească pentru achiziții în moneda din țara lor de origine, atât pentru vacanțe cât şi pentru deplasări în interes de afaceri.

- Clienții dumneavoastră vor ști exact cât au cheltuit, în moneda din țara lor de origine, fără a fi nevoie să facă vreo conversie valutară.

Nu există costuri de configurare sau taxe recurente. Noi vă vom oferi tot ce aveți nevoie pentrua a livra clienților dumneavoastră această opțiune de plată. Întreg procesul este clar și ușor atât pentru casier cât și pentru titularul cardului.

- DCC este complet automatizat și aplicația instalată, iar POS lucrează în locul dumneavoastră.

După finalizarea tranzacției, posesorul cardului primește o chitanță care arată valoarea tranzactiei de vânzare în moneda din țara lor de origine, cursul de schimb și suma finală percepută în moneda țării emitente a cardului.

În plus, de fiecare dată când un client realizează o achiziție în moneda din țara lor de origine, veți primi un comision DCC și veți vedea acest lucru în extrasul dumneavoastră de cont. Astfel, veți reduce costurile dumneavoastră operaționale și vă veți creşte profitul.

AVANTAJE PENTRU DUMNEAVOASTRĂ

- DCC creează un flux de venituri nou și continuu
- Vă oferă un avantaj competitiv pe piață
- Nu există costuri de configurare sau taxe recurente
- Vă ajută să vă dezvoltați afacerea prin atragerea posesorilor de carduri internaționale

AVANTAJE PENTRU CLIENTUL DUMNEAVOASTRĂ

- Înțelegerea clară a sumei exacte care urmează să fie percepută în moneda din țara lor de origine a clientului
- Ușor de utilizat- aplicatia POS face toate operațiunile, oferind în același timp o experiența normală de cumpărături
- Turiștii veniți în scopuri de afaceri beneficiază de reconciliere mai facilă a cheltuielilor
- Se utilizează cursurile de schimb actuale
- Suma prezentată la momentul vânzării este suma exactă cu care clientul va fi taxat pentru achiziție
- Nu există alte taxe necomunicate

Terminalul POS are opțiunea DCC activată și va detecta automat dacă cardul clientului este eligibil pentru DCC. Le puteți oferi apoi titularilor de card opțiunea de a plăti în moneda din țara lor de origine sau în RON. Rețineți faptul că clientul Dumneavoastră trebuie să aibă posibilitatea de a face o opțiune fără echivoc, dacă vrea să efectueze tranzacția în valuta națională sau în orice altă valută propusă.

Suma din contul titularului de card se debitează în moneda din țara lor de origine, deci, titularul nu va fi împovărat cu alte comisioane de conversie valutară la banca sa emitentă. În contul dumneavoastră bancar se va adăuga suma în RON, ca să nu fie necesar să țineți conturi în valută străină.

Monede acceptate

EUR, PLN, HUF, GBP, AED, NOK, CAD, SEK, CHF, DKK, CZK, AUD, MXN, JPN, USD, MDL, RUB

Oferiți-i clientului Dumneavoastră toate opțiunile disponibile și transparență

Conform directivelor organizatiilor de carduri Visa și Mastercard, fiecare titular de card care poate beneficia de serviciul DCC trebuie să fie informat cu privire la faptul că DCC este un serviciu opțional și că are posibilitatea de a plăti în RON, dacă dorește acest lucru. RON rămâne moneda implicită pentru orice tranzacție. Când un card eligibil este identificat de către POS, titularului de card i se oferă opțiunea de a decide plata în moneda din țara de origine. Moneda din țara de origine a titularului de card va fi confirmată înainte de a se acorda autorizarea. Toate informațiile DCC vor fi puse la dispoziția titularului de card înainte de finalizarea tranzacției. Aceste informații vor fi puse la dispoziția titularului de card pe ecranul POS-ului și pe chitanță la finalizarea tranzacției DCC.

Cursul de schimb

Cursul de schimb este furnizat și stabilit zilnic de către Global Payments. Acesta este folosit pentru tranzacțiile DCC de pe POS-ul dumneavoastră.

Cursul de schimb aplicat unei tranzacții DCC este furnizat titularului de card de către POS, înainte de finalizarea vânzării. Apoi acesta este tipărit clar pe toate chitanțele aferente tranzacției.

Rambursarea banilor

Pentru prelucrarea procesului de rambursare a banilor la tranzacția DCC, va trebui să introduceți suma în RON și ulterior, după solicitare, să alegeți opțiunea DCC. Verificați chitanța pentru tranzacția inițială, pentru vă asigura că a fost procesată ca DCC.

Datorită diferențelor de curs de schimb, suma finală poate fi rambursată titularului de card, diferită de valoarea tranzacției inițiale în valuta lui națională. Va trebui să îl informați despre această realitate pe titularul de card, simultan cu procedura de procesare a rambursării banilor.

Chargeback-urile

Dacă plata DCC este returnată, Visa sau Mastercard vor efectua conversia sumei din moneda din țara de origine a titularului de card în RON, înainte de a o debita din contul dumneavoastră bancar.

Datorită diferențelor de curs valutar, plata returnată la final poate fi diferită de valoarea tranzacției inițiale efectuate în RON. Vă vom informa în scris cu privire la detaliile oricăror sume returnate înainte de debitarea contului dumneavoastră bancar.

Vă vom informa în scris despre detaliile referitoare la orice proces de chargeback care este aplicat în contul Dumneavoastră bancar.

Pre-autorizarea

DCC se poate aplica tranzacțiilor de pre-autorizare atunci când un titular de card se înregistrează (la hotel sau la compania de închirieri auto). Cursul actual de schimb folosit în DCC și suma în valuta DCC trebuie să fie afișate titularului de card.

Titularul de card trebuie informat în mod clar faptul că valoarea finală a cursului de schimb DCC și valoarea DCC în moneda sa din țara de origine se va stabili atunci când tranzacția se procesează achitarea serviciului, ceea ce va implica anularea tranzacției și reluarea procesului de tranzacționare.

Vă rugăm să ne contactați în legătură cu cererea privind alte informații, dacă sunteți interesați să oferiți clienților Dumneavoastră serviciul DCC (datele de contact sunt menționate la pag. 52).

MULTICURRENCY - TRANZACȚIILE ÎN VALUTĂ STRĂINĂ

Înainte de începerea acceptării plăților cu cardul care permite clienților să efectueze tranzacții în câteva valute, veți avea nevoie de acordul nostru prealabil, în scris. Pentru efectuarea tranzacțiilor de vânzare și rambursarea banilor în valută străină puteți accepta cardurile Mastercard Credit, Visa Credit, Debit Mastercard, Visa Debit, Visa Electron, V PAY și Maestro.

Putem aranja în așa fel pentru Dumneavoastră, încât veți putea încasa plățile în valută străină, cum sunt euro, dolari americani. Puteți să selectați opțiunea ca toate tranzacțiile Dumneavoastră în valută străină să fie atribuite direct în contul rezervat în valută străină. Sumele adăugate vor fi grupate în funcție de valută, astfel că pentru toate tranzacțiile în valuta respectivă vi se va adăuga o sumă și este necesar să aveți un cont bancar special pentru fiecare valută acceptată. În caz contrar, tranzacția respectivă în valută străină vi se va adăuga în contul administrat în RON.

Dacă doriți să aflați mai multe informații despre acceptarea tranzacțiilor în valută străină, vă rugăm să ne contactați la numărul menționat la pag. 52.

CONECTAREA TERMINALULUI LA CASA DE MARCAT (ECR)

Terminalele pe care le oferim permit conectarea la sistemul de casa de marcat . Protocolul de comunicare dintre cele două dispozitive dă posibilitatea comandării la distanță a funcțiilor terminalului și a conducerii procesului de plată direct de la dispozitivul conectat. Se poate conecta la terminal prin intermediul interfeței RS232, USB sau prin intermediul TCP/IP. Pe întreaga perioadă de implementare a protocolului de comunicare suntem gata să vă oferim asistență tehnică completă, inclusiv eventualul împrumut al terminalului de testare.

Pentru mai multe informații vă rugăm să nu ezitați să îl contactați pe reprezentantul nostru comercial care vă oferă cu plăcere informațiile detaliate.

BACȘIȘURILE

Bacșișul este suma suplimentară adăugată pentru tranzacție de către titularul de card, spre exemplu, dacă titularul de card plătește nota în restaurant.

Informații detaliate le regasiti în Manualul utilizatorului aferent terminalului Dumneavoastră.

CASH BACK-ul

Serviciul CASH BACK dă posibilitatea titularului de card să primească numerar, simultan cu achiziționarea bunurilor sau serviciilor. Titularul de card plătește o sumă mai mare decât prețul bunurilor/serviciilor și suma excedentară o primește în numerar de la comerciant. Acest serviciu este acordat titularilor de carduri care au cardurile emise de banca care funcționează pe piața românească și are certificare pentru acest serviciu.

Acest serviciu este disponibil doar pentru cardurile Visa, Visa Electron, Mastercard și Maestro. Condiția posibilității de utilizare a serviciului CASH BACK este achiziția de bunuri sau servicii. Retragerea de numerar este admisă până la valoarea maximă de 200 RON.

Instrucțiunile care arată cum se realizează tranzacțiile de acest tip le găsiți în Manualul utilizatorului pentru terminalul Dumneavoastră de plată.

ACCEPTAREA CARDURILOR PENTRU BONURILE DE MASĂ

Societatea noastră oferă posibilitatea acceptării tuturor cardurilor emise pentru bonurile de masă la terminalele de plată livrate de societatea noastră.

Pentru mai multe informații nu ezitați să îl contactați pe reprezentantul dumneavoastră comercial.

ELEMENTELE SPECIFICE DE ACCEPTARE A CARDURILOR DE PLATĂ ÎN SECTOARELE SELECTATE[3]

TRANZACȚII ÎN HOTELURI ȘI COMPANII DE ÎNCHIRIERI AUTO

Operatorii rețelelor de carduri de plată au reguli specifice pentru aceste tranzacții. Această secțiune prezintă informații cu privire la proceduri, care trebuie urmate în cazul în care beneficiați de aceste tranzacții. Terminalul dumneavoastră trebuie să fie configurat pentru tranzacții de preautorizare. Dacă doriți să activați această opțiune, vă rugăm să ne contactați (datele de contact pot fi găsite la pag. 52). Procedurile detaliate de realizare a preautorizării sunt descrise în Manualul de utilizator pentru terminalul dumneavoastră de plată.

În scopurile acestei secțiuni, clienții hotelurilor și persoanele care își închiriază un autovehicul sunt considerate ca fiind titulari de card.

Pașii și procedurile de bază, care trebuie urmate în cadrul procesului de acceptare a cardurilor

- Toate documentele acordate unui titular străin de card trebuie să fie bilingve (română/engleză).
- În cazul unei rezervări sau anulări (inclusiv rezervări sau anulări prin Internet), comerciantul trebuie să asigure consimțământul titularului cardului de plată cu condițiile rezervării.
- Comerciantul are obligația de a păstra toată corespondența cu titularul cardului pentru a o prezenta ulterior băncii, în scopul soluționării unor eventuale tranzacții litigioase (reclamații).

Rezervări

În cazul unei rezervări, informați titularul cardului:
– despre prețul cazării sau prețul pentru închirierea autovehiculului și comunicați-i numărul rezervării

– despre detaliile rezervării

– despre termeni și condiții

– despre condițiile anulării și eventual despre numărul de anulare a rezervării.

Pentru primirea de rezervări pentru hoteluri și companii de închirieri auto, asigurați-vă că ați obținut:
– numele titularului de card,

– adresa și numărul de telefon,

– numărul cardului de plată al acestuia, data începerii valabilității a cardului (dacă este disponibilă) și data încetării valabilității,

– acordul pentru utilizarea cardului la plată

– acordul cu termenii și condițiile

– acordul cu prețul total, care va fi perceput în ziua creării rezervării.

În cazul în care acceptați o rezervare a camerei prin intermediul cardului Mastercard sau Visa, trebuie să garantați că veți acorda cazare alternativă la același standard sau la standarde mai bune, pentru care nu veți percepe o altă taxă în plus, în cazul în care cazarea rezervată va deveni indisponibilă.

Rezervarea garantată

Rezervarea garantată este rezervarea fără încasarea imediată a sumei de către comerciant. Comerciantul va asigura rezervarea pentru titularul cardului și îi va reține cazarea până în data planificată a sosirii. Titularului de card trebuie să i se acorde un termen de 24 de ore de la primirea confirmării rezervării pentru anularea gratuită a rezervării. Tranzacția este realizată abia în prezența titularului de card.

Rezervarea cazării cu Advance Deposit

În cazul în care hotelul permite rezervarea cu posibilitatea Advance Deposit (avans nerambursabil), această opțiune trebuie să fie specificată în condițiile rezervării, cu care Titularul cardului trebuie să-și dea acordul.

[3] Această secțiune se referă şi la comercianți, care în baza unei autorizații speciale din partea societății noastre au posibilitatea de a efectua tipuri de tranzacții corespunzătoare (de ex. preautorizări)

Comerciantul este obligat ca pe chitanța emisă de terminal să specifice „Advance Deposit" în loc de semnătura titularului de card.

Înregistrare (check-in)

- La sosire, solicitați titularul de card să semneze formularul de înregistrare, în care este prevăzut că titularul vă autorizează pentru retragerea banilor de pe cardul acestuia. Verificați dacă semnătura corespunde cu semnătura de pe card.
- Ar trebui să fie efectuată preautorizarea.
- Informați titularul de card despre mijloacele financiare, pe care le-ați preautorizat, și explicați-i cum ați ajuns la această sumă (de exemplu, prin includerea duratei cazării/închirierii, prețul camerei/prețul pentru închiriere, taxe aferente, taxe pentru servicii și taxe pentru kilometri)

Plecare (check-out)

- Cu ajutorul tastelor pe terminal selectați Meniu-Tranzacții- Preaut. finalizare, trageți sau introduceți cardul, introduceți suma inițială preautorizată, codul de autorizare și codul de identificare de pe bonul de preautorizare și procedați conform instrucțiunilor de pe terminalul dumneavoastră de plată.
  Este posibil să fiți nevoiți să efectuați o autorizare suplimentară, în cazul în care suma finală depășește:
  – limita dumneavoastră de autorizare
  – suma valorilor preautorizate anterior (la carduri Visa este permisă o toleranță de plus 15%, la Mastercard nu se admite nicio toleranță). Obțineți autorizația doar pentru diferența dintre suma sau sumele preautorizate și suma finală.
- Acolo unde este posibil, încercați ca suma finală să fie achitată în prezența titularului de card și realizați tranzacția cu aplicarea verificării prin PIN.
- Nu uitați să anulați toate codurile de autorizare nefolosite, dacă ați depășit suma preautorizată cu mai mult de 15% în cazul tranzacției cu cardul Visa.
- Nu sunteți autorizați să păstrați codul de securitate al cardului (CSC). În cazul în care ați păstrat această informație și acest fapt va fi depistat ulterior, organizatiile de carduri pot aplica amenzi in raport cu cu reglementarile în vigoare.
- Organizația de carduri Mastercard solicită ca suma autorizată să fie aceeași cu valoarea totală transmisă spre procesare.

Anularea rezervării

Titularul cardului trebuie să cunoască condițiile pentru anularea rezervării din momentul creării rezervării. În general, trebuie aplicate următoarele reguli:

- Rezervările garantate sunt ținute până în ziua următoare după data de sosire planificată.
- Termenul pentru anularea rezervării este ora 18:00 (ora locală) în ziua planificată pentru sosire.
- Dacă veți stabili un termen anterior orei 18:00 (ora locală) în ziua planificată pentru sosire, comunicați acest fapt titularului de card.
- Comunicați titularului de card în scris data, ora termenului și regulile pentru anularea rezervării.
- Comerciantul nu poate solicita ca și condiție de anulare gratuită termene mai lungi de 72 de ore înainte de sosirea clientului. În cazul stabilirii unui termen mai lung de 72 de ore înainte de sosire, reclamația titularului de card este considerată ca fiind justificată.
- În cazul în care rezervarea nu este valorificată, sau anulată în timp util, titularului de card i se percepe prețul pentru prima noapte (incl. TVA), și anume NO SHOW
- Comerciantul trebuie să acorde titularului de card codul rezervării anulate.

NO SHOW

Tranzacția de tipul NO SHOW servește pentru taxarea suplimentară a serviciului, de ex. titularul cardului își comandă un serviciu (rezervarea camerei la hotel / comandă de închiriere vehicul la compania de închirieri auto) și nu îl anulează, sau nu îl anulează în timp util. În cazul în care are loc o astfel de situație, conform regulilor organizațiilor de carduri, comerciantul este autorizat de a percepe ca despăgubiri prețul pentru o noapte/o zi.

Condiții:
- Comerciantul trebuie să informeze în scris titularul de card cu privire la taxare, prin fax sau email.
- Comerciantul trebuie să aibă informații despre card (numărul cardului, valabilitatea cardului).
- Comerciantul trebuie să aibă comanda scrisă de bunuri sau servicii.
- Comerciantul trebuie să aibă dreptul pentru taxare suplimentară scris în condițiile sale pentru prestarea de servicii.
- Cu ajutorul funcției „Vânzare", comerciantul va efectua tranzacția pe terminalul de plată, iar în locul rezervat pentru semnătură va scrie lizibil cu font italic „NO SHOW" (resp. „N.S.").

Alte comisioane

Hotelurile nu sunt autorizate să procedeze la procesarea tranzacției asociate cu „alte comisioane" pentru pierdere, furt sau deteriorarea dotărilor hotelului fără acordul titularului de card. Aceste comisioane suplimentare nu sunt garantate și pot fi debitate din contul dumneavoastră în cazul în care titularul de card va reclama cu succes o astfel de tranzacție, cauzând societății dumneavoastră pierdere financiară.

Companii de închirieri auto: Doar societatea Visa permite clientului de a percepe sume retroactive sau modificate în urma deteriorării vehiculului închiriat, pentru combustibil, asigurare, parcare, amenzi, taxe pentru închiriere și taxe fiscale. Însă trebuie să prezentați toate actele de mai jos:
- copia contractului de închiriere
- estimarea valorii daunelor de la o unitate, care este autorizată pentru a efectua reparații în țara în care își are sediul compania de închirieri auto
- un eventual proces-verbal de la poliție privind accidentul
- documentația conținând acordul titularului de card cu faptul că va achita daunele cu cardul său Visa
- orice altă documentație relevantă disponibilă, care dovedește responsabilitatea titularului de card pentru daunele produse
- copia poliței de asigurare a autovehiculului, în cazul în care solicitați ca titularul de card să plătească asigurarea, a cărei valoare va fi scăzută din valoarea daunelor achitate. În loc de polița de asigurare a companiei dumneavoastră de închirieri auto puteți prezenta copia contractului de închiriere vehicul, care confirmă că titularul de card este de acord cu achitarea unei părți pentru acoperirea evenimentului asigurat. În acest caz, este necesar ca titularul cardului să semneze în prealabil sau să atașeze inițialele sale lângă partea contractului, unde sunt prezentate informațiile cu privire la asigurare.

Organizațiile de carduri Mastercard și Maestro nu permit ca societățile de închirieri auto să perceapă de la clienți sume retroactive sau modificate. Orice taxe pentru pierderi sau sustrageri trebuie să fie procesate separat și pentru aceste procesări trebuie să obțineți acordul titularului de card.

BIROURILE DE SCHIMB VALUTAR/CAZINOURILE

Pentru a putea primi plăți cu cardul pentru servicii de birouri de schimb sau cazinou, aveți nevoie de acordul nostru scris prealabil.

Trebuie să efectuați temeinic toate controalele cardurilor descrise în secțiunea Verificarea cardurilor (a se vedea pagina 13).

În afară de aceste controale, în cadrul realizării tranzacțiilor la un birou de schimb sunteți obligați să identificați titularul de card și să efectuați înregistrarea cu privire la actul de identitate prezentat. Cerințele exacte depind de tipul cardului folosit și vă rugăm să aveți în vedere că și aici există riscul de chargeback-uri.

La locul de tranzacționare de tipul Birou de schimb valutar/Cazinou nu este permisă efectuarea tranzacției de refund.

CREDITAREA SAU DEBITAREA PLĂȚILOR DIN CONTUL DUMNEAVOASTRĂ BANCAR

CREDITAREA PLĂȚILOR ÎN CONTUL DUMNEAVOASTRĂ BANCAR

Procesarea și decontarea tranzacțiilor

Societatea noastră oferă decontare automată a tranzacțiilor, independent de închiderile efectuate. În setarea de bază, fiecare terminal efectuează închiderea automată[4], în așa-numită fereastră orară pentru realizarea închiderii (- 30 minute până la + 30 minute de la momentul închiderii). Fereastra orară pentru închidere poate fi setată oricând între 00:00- 22:55 din diverse motive ale proceselor de decontare.

Există următoarele tipuri de închideri, care pot fi realizate:

- Închidere prematură- Dacă închiderea este realizată în afara ferestrei pentru închidere (manual), nu are nicio influență asupra procesării tranzacțiilor și servește doar pentru nevoile dumneavoastră interne. Până la realizarea închiderii automate, toate tranzacțiile următoare se includ în continuare în decontarea pentru ziua respectivă și vă vor fi decontate într-o singură sumă.

- Închidere obișnuită- Dacă închiderea este efectuată în cadrul ferestrei alocate (manuală sau automată), decontarea pentru ziua respectivă se închide și următoarele tranzacții vor fi alocate în ziua următoare.

- Închidere întârziată- Dacă închiderea este efectuată după termenul stabilit pentru fereastra închiderii (manual), toate tranzacțiile realizate până la sfârșitul ferestrei de închidere vor fi decontate în ziua respectivă. Tranzacțiile realizate de la sfârșitul ferestrei pentru închidere până în momentul realizării închiderii manuale întârziate vor fi decontate în ziua următoare.

Termene pentru procesare

Pentru obținerea unui document privind tranzacția dumneavoastră, vom înainta această tranzacție emitentului corespunzător al cardului, de la care vom solicita plata în numele dumneavoastră (a se vedea „Procesarea tranzacțiilor la pag. 8), în aceeași zi, în care ne veți înainta aceste tranzacții. În cazul în care veți înainta tranzacțiile după termenul din sistem pentru transmiterea tranzacțiilor spre procesare (care este la 22:55), sau într-o zi nelucrătoare, vom înainta aceste tranzacții emitentului de card abia în următoarea zi lucrătoare.

Termene pentru creditarea plății în contul dumneavoastră

Plata va fi efectuată în contul dumneavoastră bancar sau într-o altă modalitate stabilită în Termeni și condiții generale pentru acceptarea cardurilor de plată. De obicei transmitem mijloacele financiare în următoarea zi, după ce primim cu succes tranzacția dumneavoastră procesată electronic, cu ajutorul terminalului dumneavoastră de plată. Data la care suma va fi creditată în contul dumneavoastră depinde de banca la care este deschis contul dumneavoastră.

PORTALUL PENTRU COMERCIANȚI (MERCHANT PORTAL)

Portalul pentru clienți este un sistem destinat tuturor comercianților care acceptă carduri de plată prin intermediul Global Payments. Vă oferă un rezumat al plăților dumneavoastră, al tranzacțiilor și blocărilor și vă permite să obțineți extrase în format PDF, XLSX și alte diferite rapoarte. Aceste funcții vă pot fi utile în cazul reconcilierii plăților dumneavoastră și al controlului tranzacțiilor dumneavoastră, care au fost transmise spre procesare la Global Payments din terminalele dumneavoastră.

De asemenea, portalul vă permite accesul la informații importante din punct de vedere al timpului și sensibile din punct de vedere financiar, și vă oferă flexibilitate, pe care extrasele pe hârtie nu o permit. Toate datele sunt completate zilnic și tranzacțiile individuale sunt afișate cu toate detaliile corespunzătoare.

În timpul controlului plăților și a tranzacțiilor dumneavoastră, puteți face următoarele:

- Afișarea plăților între două intervale de timp

- Afișarea rezumatelor pentru plățile selectate

- Afișarea tranzacțiilor individuale, care creează o anumită plată

[4] În baza solicitării, se poate schimba în închidere manuală

- Deschiderea chitanțelor tranzacțiilor dumneavoastră
- Căutarea unor date financiare concrete
- Sortarea datelor în funcție de plăți individuale, data tranzacției, plată, locul de tranzacționare, sumă, terminal
- Afișarea datelor pentru unul sau mai multe locuri de tranzacționare
- Analiza datelor- exportul și salvarea datelor selectate în PC-ul dumneavoastră în format XLS și utilizarea unei aplicații destinate pentru analiza datelor.

Disponibilitatea și istoricul datelor

Datele de pe portal sunt disponibile în maxim 24- 48 de ore după închiderea contabilă a terminalului. Portalul propriu-zis este accesibil nonstop, 24 ore pe zi, 7 zile pe săptămână. Este disponibil istoricul plăților de până la 2 ani.

Puteți găsi informații detaliate cu descrierea exactă a tuturor funcțiilor disponibile în Manualul utilizatorului pentru Portalul clientului.

EXTRASE

Extrasele sunt disponibile pentru descărcare în secțiunea ‚Extrase' în Merchant Portal. Sunt disponibile pentru descărcare următoarele documente: extrase de plăți, facturi și corecții de facturi pentru închiriere de terminale, facturi storno, somații și alte diferite rapoarte. Extrasele nu sunt transmise automat la adresa dumneavoastră de email.

Formatele extraselor

- *.pdf: rezumat user-friendly al tranzacțiilor încheiate, care este potrivit pentru prelucrare manuală- încărcarea în sistemul contabil nu este posibilă
- .flat, *.xml: potrivit pentru prelucrare electronică, transmitere prin email, SFTP sau pe portalul comerciantului. Este necesară instalarea unui software contabil adecvat. Pentru prelucrare manuală a acestui format, acesta se poate deschide în programul MS Excel.
- Merchant- aplicație pe Internet, care permite vizualizarea plăților, a tranzacțiilor și a autorizărilor, permite generarea de fișiere în format .pdf sau .xlsx

Tipurile extraselor

Detaliat- cuprinde informațiile de bază și un rezumat complet al tuturor tranzacțiilor procesate într-o perioadă de timp definită. Tipul recomandat

Frecvența extraselor
- Formatul .pdf

– Zilnic
– Săptămânal
– Lunar

- Formatul .xml, .flat

– Zilnic

TRANZACȚIILE RESPINSE

În cadrul procesului realizat de noi de verificare a tranzacțiilor, respingem și returnăm toate tranzacțiile care nu au trecut de verificare, de exemplu tranzacțiile realizate cu un card expirat. Tranzacțiile respinse vă vor cauza pierdere financiară.

Înainte de aceasta, verificăm detaliile tranzacției în sistemele noastre. În cazul în care găsim erori, acestea vor fi corectate. Dacă problema nu va fi rezolvată, vă vom informa printr-o scrisoare/email și suma creditată în contul dumneavoastră va fi ajustată în mod corespunzător.

În cazul în care are loc respingerea întregului fișier cu tranzacții, vă vom contacta telefonic și vă vom informa cu privire la măsurile corective, pentru a evita situația în care în contul dumneavoastră nu va fi creditată nicio sumă financiară.

COMISIOANELE PENTRU SERVICII

Este vorba de o sumă, pe care sunteți obligați să o achitați pentru serviciile prestate de noi de procesare a tranzacțiilor realizate cu cardul de plată. Comisioanele sunt calculate cel mai des ca un procent din suma tranzacției dar pot fi aplicate si alte scheme de comisionare in raport cu cele stabilite prin conditiile contractuale.

Informații detaliate despre comisioanele pentru servicii le puteți găsi în Cererea dumneavoastră de acceptare a cardurilor de plată.

RECONCILIERE

Recomandăm cu fermitate să efectuați reconcilierea contului dumneavoastră bancar în fiecare lună. Vă rugăm să ne sunați sau trimiteți un email (informațiile de contact le puteți găsi la pag. 52), dacă veți avea orice întrebări cu privire la datele din extrase referitoare la procesarea tranzacțiilor cu cardul de plată.

CHARGEBACK-URILE

INTRODUCERE

Prin chargeback se înțelege tranzacția pe care banca emitentă și-o reține în întregime, sau valoarea parțială a tranzacției plătite comerciantului, de regulă în baza reclamației depuse de titularul cardului de plată. Chargeback este uneori numit și „litigiu" (dispută).

Fiecare chargeback are reguli specifice, prevederi și intervale de timp, în cadrul cărora Global Payments trebuie să acționeze. Aceste reguli sunt stabilite de organizatiile de carduri Mastercard, Visa, JCB și UnionPay și prevăd pașii care pot fi urmați pentru a soluționa un caz de chargeback. Vom face tot ce este posibil în cadrul acestor reguli pentru a asigura protecția dumneavoastra împotriva chargeback-ului.

Există o serie de motive, pentru care o tranzacție poate fi reclamată și ulterior suma acesteia debitată din contul comerciantului, totuși aceste motive pot fi împărțite în cinci categorii principale:

- cerere de documentație (a se vedea „Ce este cererea de documentație?" mai jos)
- tranzacție neautorizată- titularul autorizat de card nu și-a dat acordul pentru o astfel de tranzacție și nu a participat la ea
- motive legate de autorizare- de exemplu, tranzacția depășește limita autorizată și a fost finalizată fără autorizare (a se vedea pagina 19), autorizarea a fost respinsă etc.
- eroare la procesare- de exemplu, procesare dublă a tranzacției
- bunuri sau servicii anulate/returnate- titularul cardului a anulat comenzile sau a returnat bunurile și nu i-au fost restituiți banii, restituirea banilor nu a fost procesată sau banii restituiți nu au fost creditați pe același card, din care au fost retrași inițial (a se vedea pagina 22)
- bunuri/servicii nelivrate- de exemplu, în cazul livrării întârziate a bunurilor sau a serviciilor, sau în cazul livrării bunurilor incorecte.

Vă vom informa întotdeauna despre chargeback printr-o scrisoare sau email înainte să fie retrase sumele aferente din contul dumneavoastră. De faptul dacă vom putea să vă protejăm față de chargeback depinde dacă tranzacția în cauză a fost în totalitate în conformitate cu regulile stabilite de organizațiile Mastercard, Visa, JCB, sau UnionPay. Acolo unde va fi posibil, de exemplu atunci când tranzacția a fost autentificată prin citirea cipului și introducerea de PIN, vă vom apăra automat față de chargeback. În cazul în care vom solicita de la dumneavoastră alte informații/documentație, veți primi de la noi o solicitare scrisă. Chargeback (suma litigioasă) va fi perceput abia după finalizarea întregului proces de chargeback.

În cazul în care vă vom contacta în scris cu solicitări de informații, este foarte important să furnizați informațiile solicitate, într-un format clar și în termenul stabilit în scrisoarea noastră. În caz contrar, putem avea impedimente în apărarea dumneavoastră față de chargeback în cadrul intervalului de timp posibil.

Solicitările pentru furnizarea documentației pot fi transmise până la 90 de zile după ce tranzacția a fost debitată din contul titularului de card sau după ce serviciul respectiv a fost recepționat. Cu toate acestea, în unele cazuri, de exemplu atunci când a fost vorba de o fraudă, documentele pot fi solicitate până la doi ani după data tranzacției. De aceea, este crucial să puteți furniza cu ușurință această documentație. Nu uitați că datele de pe carduri trebuie să fie păstrate în condiții de securitate (a se vedea pag. 41 privind „Securitatea datelor")

Vă rugăm să ne contactați (datele de contact le puteți găsi la pagina 52), dacă doriți să discutați cu noi referitor la scrisoarea care anunță un chargeback sau dacă nu sunteți siguri ce documentație vi se solicită.

CE ESTE CEREREA DE DOCUMENTAȚIE?

Cererea de documentație este depusă atunci când titularul cardului ridică o întrebare referitoare la o tranzacție efectuată cu cardul de plată. Adesea este din cauza faptului că titularul cardului nu își amintește că ar efectua tranzacția respectivă.

Cererea de documentație nu este chargeback. Aceasta înseamnă că nu vom retrage nicio sumă din contul

dumneavoastră. Totuși, cererea de documentație poate rezulta în chargeback, dacă informațiile pe care emitentul cardului le obține de la noi sunt ilizibile, nu sunt suficiente pentru a răspunde întrebării titularului de card, sau nu dovedesc autentificarea clientului prin intermediul cipului pe card, împreună cu verificarea PIN-ului sau autentificarea prin intermediul plății securizate prin Internet.

Este important să dați curs imediat cererii de documentație, deoarece în caz contrar, conform regulilor Mastercard, Visa, JCB și UnionPay, putem pierde dreptul de a vă apăra față de orice alte chargeback-uri ulterioare.

CUM TREBUIE SĂ EVITĂM CHARGEBACK-URILE

Tranzacții la care cardul este prezent (CP)

Cardurile cu cip și terminalele cu introducerea PIN-ului au progresat semnificativ în prevenirea de fraude cu carduri și în perioada actuală reprezintă un standard.

Standardele operatorilor de rețele de carduri de plată solicită ca tranzacțiile CP, unde este prezentat un card cu cip cu PIN, să fie efectuate prin citirea cipului și introducerea PIN-ului în terminal. Utilizarea benzii magnetice în locul cipului este permisă dacă după introducerea cipului, terminalul vă invită să utilizați banda magnetică.

Totuși, sunt folosite multe carduri valabile, care nu au cip și trebuie trase prin cititor și citite datele de pe banda magnetică. După efectuarea acestei operațiuni se poate întâmpla ca pentru verificarea tranzacției va trebui să folosiți semnătura titularului de card. De asemenea, există o serie de carduri, care au cip, dar solicită pentru verificare doar semnătura titularului de card. Unele din aceste carduri au fost emise în străinătate sau anumitor titulari de card, care nu pot folosi PIN-ul.

Cea mai bună metodă de minimizare a riscului de chargeback-uri la tranzacții CP este de a urmări cu atenție solicitările, care apar pe terminalul dumneavoastră. Dacă terminalul autorizează plata și solicită semnătura titularului de card, această procedură ar trebui permisă luând în considerare faptul că trebuie efectuate controalele obișnuite pentru tranzacțiile verificate cu semnătură (a se vedea pagina 12).

Tranzacții la care cardul nu este prezent (CNP)

În mediul CNP este important să aveți în vedere că sunteți expuși unui risc mai mare de chargeback-uri. Dacă veți urmări punctele prezentate mai jos și vă veți ghida după informațiile specificate în secțiunea „Cum se poate reduce riscul de fraudă” de la pag. 45, acest risc va fi redus la nivelul minim:

- În cazul în care clientul solicită ridicarea bunurilor din magazin, realizați tranzacția la ridicare, și anume ca tranzacție la care cardul este prezent, cu ajutorul dispozitivului dumneavoastră la locul de tranzacționare.

- Trimiteți întotdeauna bunurile cu poștă recomandată sau poștă specială, sau prin intermediul unei societăți de transport de încredere și sigure. Insistați asupra faptului că trebuie emisă o dovadă de livrare, care trebuie semnată ulterior, dacă este posibil de către titularul cardului. Solicitați curierul să nu livreze coletul, dacă locul în care trebuie să fie livrat pare a fi gol. Vă rugăm să aveți în vedere că dovada de plată propriu-zisă nu este suficientă pentru a vă proteja față de chargeback.

- Niciodată nu predați bunurile terților, cum ar fi de exemplu șoferi de taxi sau mesageri.
- Acordați o atenție mai mare tranzacțiilor, la care adresa de facturare diferă de adresa de livrare solicitată. Evitați livrările la adresele care diferă de adresa titularului de card, precum hoteluri, Internet cafe-uri și adrese ale altor persoane, la care se află destinatarul.

- Procedați cu atenție în cazul cerințelor de livrare a doua zi, a cerințelor de modificare rapidă a adresei de livrare, a apelurilor telefonice în ziua livrării, în care cumpărătorul solicită o anumită oră de livrare.

- De asemenea, acordați o atenție sporită cazurilor în care comanda a fost plasată dintr-un cont de email, în care numele clientului nu este cuprins în niciun fel în adresa de email.

- Fiți suspicioși față de tranzacțiile care, având în vedere tipul afacerii dumneavoastră sunt neobișnuit de mari în ceea ce privește valoarea și volumul, sau vânzarea este „prea ușoară”. Experiența noastră ne spune că tocmai la aceste tranzacții este o probabilitate mare că vor fi frauduloase.

- În cazul în care restituiți bani, întotdeauna face restituirea pe același card de plată, cu care a fost efectuată tranzacția inițială.

- Țineți o bază de date cu tranzacții reclamate (chargeback-uri), pentru a putea identifica ușor formule în tranzacții frauduloase. Dacă vânzarea pare a fi „prea frumoasă pentru a fi reală", atunci probabil nu este reală. Nu vă temeți să contactați titularul cardului pentru a-i adresa întrebări suplimentare sau pentru a solicita identificare suplimentară. Clientul cinstit ar trebui să aprecieze că țineți la securitate și că încercați să protejați clienții dumneavoastră de fraude.

- Pentru tranzacții în cadrul magazinelor online, pe site-ul web ar trebui să fie implementat încă un nivel de securizare. Funcțiile Mastercard SecureCode și Verified by Visa (VbV) au fost create pentru a permite clienților de a se identifica ca fiind titularul real al cardului (a se vedea pag. 48). Pentru a putea accepta cardurile Maestro prin Internet, trebuie să suportați Mastercard SecureCode.

Majoritatea chargeback-urilor rezultă ca urmare a tranzacțiilor frauduloase. Dacă finalizați o tranzacție care pare a fi frauduloasă, o faceți pe propriul risc. În cazul în care tranzacția a fost finalizată, însă bunurile nu au fost transmise, încă sunteți în poziția în care puteți restitui banii clientului.

Obținerea cu succes a unei autorizări

Autorizarea tranzacției cu cardul de plată este modalitatea de a verifica dacă cardul nu a fost pierdut/sustras și dacă titularul cardului are în momentul realizării plății mijloace financiare suficiente în contul său.

Autorizarea cu succes nu este verificarea identificării Titularului de card și prin urmare nu este nici garanția că va fi plătită.

Dovadă de preluare a bunurilor

A se vedea capitolul „Livrarea bunurilor" la pag. 38 pentru mai multe informații cu privire la livrarea bunurilor și importanța de a obține dovada de livrare. Vă rugăm să aveți în vedere că dovada propriu-zisă nu este dovada suficientă, care ar împiedica chargeback-ul.

Dacă finalizați vânzarea de bunuri sau servicii în afara punctelor dumneavoastră de vânzare, recomandăm să folosiți un terminal mobil pentru validarea tranzacției. În cazul în care tranzacția este reclamată ulterior, vom solicita o dovadă a faptului că titularul cardului și cardul au fost prezenți în momentul tranzacției.

Primirea avansului- Bunurile sunt comandate, însă nu sunt livrate imediat

Uneori se vorbește despre „livrare amânată" și de obicei se folosește în cazul tranzacțiilor, unde nu este posibilă livrarea imediată a bunurilor achiziționate, de exemplu, atunci când este vorba de o piesă mare de mobilier, care a fost realizată la comandă. În aceste cazuri puteți solicita ca titularul cardului să realizeze achiziția în două tranzacții separate, când în prima tranzacție va depune un avans, iar prin cea de-a doua va achita diferența de plată.

În cazul în care vânzarea este realizată prin această metodă, este important ca ambele tranzacții să fie procesate separat, iar cea de-a doua tranzacție acceptată să nu fie procesată până nu au fost expediate bunurile. În cazul în care veți procesa tranzacția acceptată, iar diferența de plată a fost achitată înainte ca bunurile să fie expediate, titularul cardului poate percepe aceasta ca fiind „nelivrarea bunurilor" și poate solicita de la emitentul cardului să-i fie restituită suma tranzacției cu ajutorul chargeback-ului.

Regulile organizațiilor de carduri de plată prevăd că tranzacția acceptată prin care a fost achitat avansul poate fi înaintată spre procesare înainte de expedierea bunurilor sau a serviciilor. Însă tranzacția acceptată, prin care a fost achitată diferența de plată nu poate fi înaintată spre procesare până nu au fost expediate bunurile.

Neprimirea bunurilor sau neprestarea serviciilor

- Nu procesați tranzacția cu cardul de plată până nu a avut loc expedierea bunurilor sau prestarea serviciilor.

- Nu procesați nicio tranzacție cu cardul de plată, unde titularul cardului a plătit deja bunurile sau serviciile cu ajutorul unei alte metode de plată.

- Solicitați ca titularul cardului să semneze dovada dumneavoastră de livrare sau de prestare a serviciilor, după ce ați finalizat serviciile respective.

- În cazul în care nu puteți livra bunurile și serviciile integral, informați permanent titularul de card cu privire la toți pașii dumneavoastră.

- În cazul în care ați taxat titularul de card pentru bunuri, pe care încă nu le puteți expedia, realizați doar o tranzacție parțială. Obțineți autorizarea pentru valoarea bunurilor, pe care le puteți expedia.

Bunurile nu corespund descrierii

- Este obligația dumneavoastră să asigurați ca bunurile comandata de către titularul cardului să fie livrate exact așa cum sunt descrise în catalogul dumneavoastră, sau în cadrul reclamei dumneavoastră. În cazul în care nu puteți livra bunurile cu specificațiile exacte, inclusiv culoare, mărime, calitate și cantitate, trebuie să atenționați titularul de card cu privire la modificări și să solicitați aprobarea acestuia în ceea ce privește varianta modificată.

- Bunurile ar trebui să fie livrate la timp și ar trebui să fie adecvate scopului, pentru care au fost comandate: de exemplu, nu pot fi considerate acceptabile biletele de teatru, care au sosit după data spectacolului.

- În cazul în care titularul de card primește bunurile și acestea sunt deteriorate, sparte sau inadecvate în alt fel scopului dorit, titularul cardului va avea dreptul să solicite de la dumneavoastră restituirea sumei tranzacției (chargeback).

- În cazul în care titularul de card vă returnează bunurile, aveți obligația de a restitui titularului imediat suma integrală, pe care a plătit-o pentru bunuri.

Alte motive pentru chargeback

Mai jos sunt prezentate alte câteva motive obișnuite pentru chargeback: Nu este vorba de o lista exhaustivă și în condițiile în care veți lua în considerare recomandările specificate în aceste Instrucțiuni pentru comercianți, ar trebui să fiți capabili să evitați chargeback-urile.

- tranzacție procesată pe un card expirat

- sumă incorectă a tranzacției- titularul cardului a fost taxat cu mai mult decât a preluat în realitate sau decât a fost informat.

- moneda incorectă a tranzacției- tranzacția a fost înregistrată într-o altă monedă decât cea pe care titularul de card a aprobat-o activ.

- clientul nu și-a dat acordul activ cu contabilizarea ulterioară a tranzacției suplimentare

PCI DSS/ACCEPTAREA CARDURILOR DE PLATĂ ÎN CONDIȚII DE SECURITATE

În momentul în care acceptați un card de plată pentru realizarea unei tranzacții fără numerar, trebuie luată în considerare importanța datelor, pe care le colectați în cadrul tranzacției de plată și protecția corespunzătoare a acestor date.

În cazul unui incident de securitate, vă expuneți riscului de pierderi financiare și prejudiciere a reputației afacerii dumneavoastră.

Standardul Payment Card Industry Data Security Standard (PCI DSS) cuprinde reguli obligatorii la nivel internațional privind manipularea în condiții de securitate a datelor referitoare la cardul de plată și a datelor tranzacției, care au fost stabilite de societățile de carduri cu obiectivul de a majora nivelul de securitate al acestui tip de date.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

PCI DSS este un ansamblu de cerințe complexe pentru securizarea datelor referitoare la clienți de pe cardurile de plată. Printre acestea se numără cerințele pentru administrarea securizării, directive, proceduri, arhitectura de rețea, formatul software-ului și alte măsuri cheie de protecție.

Obiectivul standardului este de a ajuta societățile în protejarea datelor despre clienți de pe cardurile de plată în businessul zilnic. Datele personale, sensibile, salvate pe card sau în card reprezintă cheia pentru realizarea tranzacției. Dacă nu veți proteja aceste date în mod corespunzător, se poate întâmpla ca hackerii, care vor descoperi locurile vulnerabile ale sistemului dumneavoastră și vor reuși să spargă sistemul, să sustragă aceste date. Aceste date sunt foarte valoroase pentru ei, deoarece le pot folosi în mod abuziv pentru finanțarea altor activități ilegale.

Este vorba de un pericol foarte real. Fiecare comerciant, indiferent de cât de mare este afacerea lui, este expus riscului de scurgeri de date. O consecință poate fi amendă aplicată de operatorul rețelei de carduri de plată, deoarece datele clientului nu au fost securizate suficient de eficient și conform standardelor PCI DSS. Aceste amenzi încep cu suma de 5.000 euro, însă în funcție de împrejurările concrete pot fi mult mai mari.

Proceduri recomandate

În principiu, conformitatea cu standardul PCI DSS înseamnă că manipulați datele financiare de pe cardurile de plată ca și cum ar fi vorba de numerar. Ar trebui să asigurați că datele sunt manipulate în condiții de securitate maximă posibilă, respectând cel puțin următoarele:

- nu veți furniza informațiile de pe cardurile de plată altor persoane, în afară de noi
- veți limita accesul angajaților dumneavoastră la datele de pe cardurile de plată.

În niciun caz nu păstrați următoarele informații:

- datele complete salvate pe banda magnetică sau în cip- cunoscute de asemenea ca Track 2 Data – de exemplu, valoarea de verificare a cardului (Card Verification Value, CVV, Batch Code), codul de validare a cardului (CVC) și valoare de verificare PIN (PIN Verification Value, PVV).
- Codul de validare a cardului (CVC – trebuie să fie șters imediat după ce ați autorizat tranzacția, chiar și în cazul tranzacțiilor CNP, precum comenzile prin poștă sau telefon (MOTO), sau tranzacțiile pe Internet nesecurizate.

Este foarte important să implementați următoarele proceduri:

- păstrați doar acele date sensibile, care sunt indispensabile pentru afacerea dumneavoastră, pe perioada strict necesară
- păstrați toate materialele, care conțin informații despre carduri (de ex. chitanțe ale tranzacțiilor) într-un spațiu sigur, încuiat, pe perioada strict necesară
- distrugeți sau ștergeți toate mediile care conțin date învechite din tranzacții, care includ informații despre titularul de card, fără întârziere
- asigurați ca toate persoanele terțe, care procesează sau salvează pentru dumneavoastră datele sensibile, sau acele persoane, cu care sunteți în discuții cu privire la aceste servicii, să confirme că îndeplinesc

standardul PCI DSS și sunt înregistrate pe site-urile societăților de carduri (Visa, Mastercard).

- păstrați chitanțele tranzacțiilor într-un loc sigur și pe perioada stabilită de legislația locală de la livrarea bunurilor sau serviciilor, iar după expirarea acestei perioade asigurați distrugerea lor sigură

- păstrați datele despre titularii de carduri doar dacă este strict necesar; în orice caz însă, aceste date trebuie să fie stocate în siguranță și trebuie să fie criptate.

Indiferent dacă creați, revizuiți sau proiectați singuri sisteme de înregistrare a plăților, sau le achiziționați prin intermediul terților, care stochează, procesează și transmit datele sensibile de pe cardurile de plată, este important să asigurați ca acest sistem și persoanele terțe corespunzătoare să respecte standardul PCI DSS. Furnizorii de servicii și aplicații, care au trecut de auditul PCI DSS și PA-DSS, sunt prezentați pe site-ul oficial al Consiliului PCI DSS https://www.pcisecuritystandards.org/.

Dacă pe echipamentul dumneavoastră POS utilizați un software disponibil pe piață, aveți obligația stabilită de operatorii rețelelor de carduri de plată de a asigura că acest software respectă standardul Payment Application Data Security Standard (PA-DSS). Utilizarea unui software, care nu corespunde acestui standard încalcă regulile stabilite de operatorii rețelelor de carduri de plată și vă expuneți astfel riscului de sancțiuni semnificative, alte cheltuieli și amenzi. De asemenea, majorați prin aceasta riscul de scurgere a datelor cu impact financiar și reputațional semnificativ asupra afacerii dumneavoastră.

Toate echipamentele furnizate de noi pentru acceptarea cardurilor de plată sunt în conformitate cu versiunea în vigoare a standardului PCI DSS. Datorită acestui lucru, afacerea dumneavoastră va putea atinge mai ușor conformitatea cu PCI DSS.

Pentru alte informații despre PCI DSS vizitați:
- http://www.pcisecuritystandards.org – acest site conține cea mai nouă versiune a standardelor PCI DSS și recomandări pentru respectarea acestor standarde

- http://www.mastercard.com/us/sdp/merchants/index.html

- http://www.Visaeurope.com/receiving-payments/security.

NIVELUL	CRITERIILE	PROCEDURILE DE VALIDARE	REALIZATE DE
1	Peste 6 000 000 de tranzacții pe an cu cardurile Mastercard și Visa	• Audit anual de securitate la sediul societății și Report on Compliance (ROC) • Scanarea trimestrială a rețelei	Evaluator de securitate calificat (QSA, Qualified Security Advisor)
2	Între 1 000 000 și 6 000 000 de tranzacții pe an cu cardurile Mastercard și Visa	• Audit anual de securitate la sediul societății (inclusiv ROC) • Scanarea trimestrială a rețelei	QSA sau evaluator de securitate intern (ISA, Internal Security Assessor)
3	Între 20 000 și 1 000 000 de tranzacții pe an într-un magazin pe Internet	• Chestionar de autoevaluare PCI anual (SAQ, Self-Assessement Quesitonnaire) • Scanarea trimestrială a rețelei	Chestionar de autoevaluare
4	Mai puțin de 20 000 de tranzacții într-un magazin pe Internet și mai puțin de 1 000 000 de tranzacții pe an	• PCI SAQ anual • Scanarea trimestrială a rețelei	Chestionar de autoevaluare

OBLIGAȚIILE DUMNEAVOASTRĂ

Respectarea Standardului PCI DSS

În cadrul Contractului privind procesarea tranzacțiilor cu cardul de plată, pe care l-ați încheiat cu noi, vi se solicită să respectați standardul PCI DSS.

Toți comercianții se vor încadra într-una din cele patru categorii de comercianți, în baza volumului de tranzacții pentru perioada din ultimele 12 luni. Următorul tabel prezintă volumul tranzacțiilor pentru fiecare nivel și metoda de validare, pe care trebuie să o folosiți.

Lista completă de QSA calificați o puteți găsi pe site-ul PCI Security Standards Council:

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

Site-ul următor oferă informații despre cum puteți deveni ISA:

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

Este necesar să ne demonstrați în mod regulat că respectați standardele PCI DSS. De aceea, vă rugăm să ne transmiteți următoarele:

- Confirmarea dumneavoastră scrisă privind respectarea standardelor:
- Attestation of Compliance (face parte din documentația SAQ) pentru comercianți, care își realizează auditul singuri, în colaborare cu ISA (anual)
- Report on Compliance (ROC) pentru comercianți, la care auditul a fost realizat de către un auditor extern (anual)
- ASV – document cu privire la rezultatul scanării rețelei (trimestrial)
- În cazul în care lucrați cu persoane terțe, copia AOC a acestei terțe persoane.

Transmiteți, vă rugăm, documentele specificate mai sus reprezentantului dumneavoastră comercial sau direct echipei PCI DSS la adresa pci@globalpayments.cz sau sunați la linia noastră de suport (datele de contact pot fi găsite la pag. 52), în cazul în care aveți nevoie de orice alte informații.

TERȚII

În cazul în care folosiți serviciile societăților terțe și acordați acestor societăți accesul la datele cardurilor și datele financiare ale titularilor de carduri pentru orice scop (de ex. procesarea tranzacției, stocarea datelor sau servicii de call center), va trebui să asigurați că și aceste terțe persoane respectă toate regulile și prevederile în domeniul securității datelor. Toți terții care stochează sau procesează pentru dumneavoastră aceste date trebuie să respecte îndeosebi standardul PCI DSS și trebuie să fie înregistrați la societățile de carduri. Pentru orice nerespectare a acestor cerințe de către societatea colaboratoare veți fi responsabili dumneavoastră, și astfel vă puteți expune unui risc nedorit de pierderi financiare.

Se solicită copia AOC a terților. Vă rugăm să o transmiteți la adresa specificată.

Domeniul turismului este un segment foarte riscant din punct de vedere al scurgerii datelor de pe cardurile de plată și a datelor private ale titularilor lor, care duc nu doar la pierderi financiare semnificative, ci și la pierderea reputației entității sau lanțului respectiv. Entitățile segmentului de turism trebuie să prezinte și AOC al furnizorului de Hotel Management System și ale societăților, care efectuează servicii pentru comerciant, de ex. rezervări, plata avansurilor etc.

CE SE ÎNTÂMPLĂ DACĂ NU OBȚINEȚI CONFORMITATEA CU PCI DSS?

În cazul în care nu veți dovedi conformitatea cu acest standard, vi se pot aplica taxe lunare pentru nerespectarea cerințelor de securitate, care sunt percepute retroactiv și sunt nerambursabile. Aceste taxe pentru nerespectarea standardului PCI DSS vor continua până nu veți obține din nou conformitatea cu PCI DSS.

Indiferent de calea pe care o veți alege pentru obținerea conformității, nu veți fi considerați ca fiind o entitate care respectă standardul PCI DSS, până nu obținem și nu raportăm statutul dumneavoastră în ceea ce privește acest aspect la organizatiile de carduri.

DACĂ SUSPECTAȚI VIOLAREA SECURITĂȚII

Dacă veți respecta procedurile recomandate mai sus și dacă veți obține conformitatea integrală cu standardul PCI DSS, veți reuși să reduceți riscul unui incident de securitate la minim. Securizarea însă nu poate fi niciodată perfectă, de aceea este indispensabil să aveți stabilit un plan de reacție imediată adaptat nevoilor afacerii dumneavoastră și astfel să știți ce pași trebuie să urmați.

În cazul în care constatați încălcarea securității în afacerea dumneavoastră (scurgerea de date), care se referă la date financiare de pe carduri de plată, sau dacă suspectați o astfel de încălcare, trebuie să efectuați următoarele măsuri:

- contactați-ne imediat la următoarea adresă de email: pci@globalpayments.cz
- nu încercați să accesați sau să modificați sistemele sparte- nu vă înregistrați în ele și nu modificați nicio parolă
- nu opriți aceste sisteme de înregistrare a plăților: izolați-le de la rețeaua dumneavoastră și deconectați toate cablurile de rețea
- păstrați toate log-urile generate și înregistrările digitale asemănătoare
- efectuați un back-up al sistemelor dumneavoastră, pentru a le păstra în stadiul actual: va simplifica cercetările ulterioare
- înregistrați pașii urmați.

În plus, ar trebui să apelați cu o cerere de consultanță profesională la un anchetator legal calificat, aprobat de PCI DSS. Lista societăților care prestează acest serviciu o puteți găsi la adresa:

www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php

CUM SE POT LIMITA FRAUDELE

Fraudele sau tranzacțiile frauduloase au devenit o epidemie globală, care este un pericol pentru toți fără excepție. Este tentant să credeți că imediat ce plata a fost autorizată, aveți siguranța că veți primi banii ce vi se cuvin. Din păcate, nu este așa.

Autorizarea nu garantează plata!

Atunci când este acordată autorizarea, prin aceasta este confirmat doar faptul că pe card sunt disponibile mijloace financiare suficiente și că respectivul card nu a fost raportat ca pierdut sau sustras- deocamdată. Proprietarul autorizat nu trebuie să știe că cineva folosește datele de pe cardul lui de plată, și astfel tranzacția se poate dovedi ca fiind frauduloasă.

Marea majoritate a plăților cu cardul este finalizată fără orice fel de probleme. Însă o singură tranzacție frauduloasă poate avea impacturi negative semnificative pentru dumneavoastră: trebuie să-i acordați timp, vă costă bani și poate deteriora reputația dumneavoastră.

Escrocii sunt inventivi, creativi și adaptabili. Pentru a avea informații mai bune despre posibile atacuri ale escrocilor, am creat o listă a celor mai dese fraude, cu care ne-am întâlnit de-a lungul colaborării cu clienții noștri.

TIPURILE DE FRAUDE, CĂRORA TREBUIE SĂ LE ACORDAȚI ATENȚIE

Utilizarea mai multor carduri și încercări respinse

Escrocii își cumpără adesea seturi de date sustrase de pe carduri sau aceste carduri propriu-zise și încearcă să facă comenzi prin telefon, fax sau online. Vor încerca fiecare set de date de pe carduri, până nu vor ajunge la acele date, care vor funcționa. Dacă veți observa respingere multiplă, comanda respectivă trebuie tratată cu vigilență.

Cerință pentru înaintarea autorizării către centrul de autorizare

Dacă în timpul realizării tranzacției, pe display-ul terminalului dumneavoastră apare mesajul „SUNAȚI CA sau „SUNAȚI AUT. VOCE", ar trebui să sunați la centrul nostru de asistență (datele de contact pot fi găsite la pag. 52), pentru a putea fi efectuate alte controale, al căror obiectiv este de a afla dacă clientul dumneavoastră este titularul real al cardului. **Niciodată** nu acceptați codul de autorizare, pe care vi-l va furniza clientul dumneavoastră, sau codul de la persoana care va suna la firma dumneavoastră și va susține că este de la centrul de autorizare. Astfel de coduri nu sunt autentice și emitentul cardului vă va putea reclama cu succes plata, în cazul în care veți folosi aceste coduri.

Vânzarea împărțită

În cazul în care are loc respingerea tranzacției cu toată suma comenzii, nu încercați să împărțiți suma în sume mai mici sau între mai multe carduri. Adesea, escrocii nu sunt conștienți de soldul de pe card (carduri), în posesia cărora au intrat, și vor solicita de la dumneavoastră să introduceți diferite sume, până se va reuși realizarea tranzacției.

Tranzacția prin intermediul benzii magnetice și a cardului falsificat

Tranzacțiile prin cip și PIN sunt tot mai dese la nivel mondial, însă până nu va fi extinsă universal utilizarea acestei tehnologii, va fi necesar ca toate cardurile să fie prevăzute în continuare cu bandă magnetică și câmp pentru semnătură.

Însă în cazul în care cardul are cip, fiți vigilenți atunci când clientul spune că cipul nu funcționează sau că și-a uitat PIN-ul.

De asemenea, aveți grijă la cardurile falsificate, pe care au fost tipărite, ștanțate sau codificate datele de pe cardul real. Majoritatea cardurilor falsificate este rezultatul unei fraude, care se numește „skimming", atunci când datele de pe un card sunt copiate fără cunoștința titularului real al cardului. „Skimming" are loc printre altele la casele magazinelor cu amănuntul, unde cardul este introdus într-un dispozitiv fraudulos, care copiază electronic datele titularului de card.

De aceea, este important ca la tragerea cardului prin cititorul terminalului dumneavoastră să aveți grijă să respectați instrucțiunile din acest document, referitoare la controlul cardurilor (a se vedea pag. 13).

De asemenea, luați în considerare alte semnale de avertizare prezentate mai jos:

- fiți atenți la cumpărături aparent întâmplătoare și nelogice, de exemplu, atunci când clientul cumpără un număr mare de bucăți identice.
- clientul nu s-a deranjat să încerce îmbrăcămintea?
- clientul este agitat și încearcă să vă distragă atenția?
- este vorba de o tranzacție cu o sumă mică, dar cu o sumă mare de Cash Back?
- suma tranzacției este imediat sub limita dumneavoastră de autorizare?

Phishing

Phishing este modalitatea prin care escrocii pot obține datele de pe card, pe care le pot utiliza ulterior pentru comiterea unei fraude în mediul CNP.

Phishing poate fi realizat cu ajutorul emailurilor, care par a fi din partea unei societăți legitime, care activează pe Internet. Aceste emailuri încearcă să înșele clienții și să-i determine să prezinte informații sensibile pe site-uri false pe Internet, create și administrate de escroci. Aceste emailuri susțin de obicei că informațiile din contul clientului nu trebuie „actualizate" sau „verificate" și îl invită pe destinatar să deschidă linkul din email, care îl redirecționează spre site-ul fraudulos. Orice informații introduse pe acest site vor fi înregistrate de acești escroci și ulterior folosite în mod abuziv în activitatea lor criminală.

De asemenea, escrocii pot contacta firma dumneavoastră și pot pretinde că sunt tehnicieni care repară terminalele, sau că reprezintă organizatiile Mastercard, Visa sau Global Payments și pot solicita informații despre ultimele tranzacții, pe care le-ați procesat. **Niciodată** nu le furnizați nicio informație.

În cazul în care vom solicita orice informații de la dumneavoastră, vom comunica cu dumneavoastră de pe adresa de email, care se va termina cu @fraudvgpe.cz. **Niciodată** însă nu vom solicita de la dumneavoastră numărul cardului.

În caz de orice suspiciuni, vă rugăm nu ezitați a ne contacta.

Adresele de email

Există două tipuri de adrese de email. Accesul la email face parte în general din pachetul de servicii preplătite ale clientului de la Furnizorul lui de servicii de Internet (ISP, Internet Service Provider). De asemenea, pot fi folosite conturile de email „gratuite", precum Yahoo, Hotmail sau Google Gmail.

Mulți clienți folosesc conturile de email „gratuite" datorită posibilității de a citi și trimite emailuri oriunde, unde este conexiune de Internet. Totuși, escrocilor le place să folosească tocmai aceste conturi „gratuite" de email, datorită anonimității, pe care le-o asigură – marea majoritate a fraudelor pe Internet a fost comisă atunci când escrocul a specificat o adresă „gratuită" de email. Sunteți îndreptățiți de a fi suspicioși, atunci când numele clientului nu este inclus în vreun fel în adresa de email.

Adresa de email propriu-zisă nu ar trebui să stea la baza hotărârii dacă o tranzacție poate fi frauduloasă. În cazul în care este folosită o adresă „gratuită" de email, trebuie efectuate alte forme de verificări.

Recomandăm clientului să trimită un email după ce a fost plasată comanda. Recomandăm cu fermitate să nu continuați cu tranzacția, dacă programul de email vă anunță că emailul nu a putut fi livrat la adresă.

Cerința de a plăti terților prin transfer bancar

Fiți suspicioși dacă un client va plasa o comandă pentru bunuri și/sau servicii și în același timp vă va solicita să acceptați plata pentru servicii suplimentare, care urmează a fi prestate de o altă societate. Apoi veți fi solicitați de către client să transferați către societatea respectivă prin transfer bancar acești bani suplimentari, pe care i-ați preluat. De asemenea, clientul vă poate oferi o sumă suplimentară în semn de mulțumire pentru faptul că l-ați ajutat. Este vorba însă de fraudă, pe care o întâlnim cel mai des la hoteluri și pensiuni.

De asemenea, fiți foarte atenți în cazul în care exportați bunuri într-o altă țară și clientul dumneavoastră vă solicită să transmiteți societății lui de transport o anumită sumă financiară prin transfer bancar. Este posibil ca societatea de transport să nu existe și comanda să fie cu o probabilitate ridicată frauduloasă.

Respingeți toate cerințele, pe care le veți primi pentru transferul plăților excedentare către terți, precum intermediari și facilitatori, prin transfer bancar.

Fraudele cu restituirea banilor

Atunci când cumpărăturile au fost făcute cu un singur card, orice restituire a banilor ar trebui efectuată pe același card. Suspiciunile sunt justificate atunci când clientul solicită restituirea banilor pe un alt card sau restituirea prin intermediul transferului bancar.

Din păcate, ne întâlnim des cu cazuri, când unul din angajați procesează tranzacția pentru restituirea banilor astfel că restituie banii pe propriul său card- așadar, asigurați-vă că aveți controlul asupra faptului cine are acces la PIN-ul de supervizor de la terminalele dumneavoastră. Asigurați să aveți implementate procedurile, care vă vor ajuta să depistați activități neobișnuite în zona de restituire a banilor.

De asemenea, în ultimul timp a fost înregistrată o creștere a numărului de fraude, în care se folosește tehnica de inginerie socială, de exemplu phishing, pentru obținerea informațiilor despre contul comerciantului, cu obiectivul de a efectua restituire frauduloasă a banilor. Cu folosirea datelor astfel obținute, escrocii pot sparge gateway-ul de plată al comerciantului sau software-ul furnizat de o terță parte, și apoi să introducă restituirea banilor în contul cardului, care a fost creat anterior cu utilizarea datelor false sau în urma furtului contului. Imediat după ce banii au fost creditați în cont, sunt rapid retrași. Aceste tranzacții pot apărea ca și când în conturile titularilor de carduri au fost restituiți bani în mod legitim pentru bunurile reclamate, însă în realitate bunurile sau serviciile nu au fost achiziționate niciodată.

Pentru a reduce riscul ca firma dumneavoastră să devină victimă a acestui tip de fraude, întotdeauna trebuie:

- să asigurați că numele dumneavoastră de utilizator și parola de cont sunt salvate în formă criptată
- să asigurați că parolele pentru gateway-urile de plată pe Internet sunt modificate în mod regulat- cel puțin la fiecare 90 de zile
- în cadrul restituirii banilor, asigurați-vă că aveți datele de la tranzacția inițială de vânzare și că restituiți banii în același cont aferent cardului
- în cazul în care dețineți un terminal mobil, asigurați-vă că este securizat pentru toate împrejurările, pentru ca escrocii să nu-l poată lua și pleca cu el
- În cazul în care ați primit un terminal nou pentru punctul de vânzare (POS), modificați imediat parola de supervizor din codul aleatoriu setat din fabrică și modificați în continuare această parolă în mod regulat.
- Informați-ne imediat dacă POS-ul dumneavoastră se pierde sau este sustras. Astfel, aceste dispozitive vor fi blocate, pentru a nu putea procesa în continuare plăți cu acestea.

CUM POT SA-MI PROTEJEZ AFACERAE MEA?

Avem o echipă motivată și hotărâtă, din care fac parte anchetatori de fraude, care utilizează instrumente de monitorizare pentru a evalua și monitoriza riscurile de fraude. Această echipă verifică formulele din tranzacțiile comerciale ale comerciantului, pentru a stabili dacă a apărut orice activitate frauduloasă, sau dacă există pericolul unei astfel de activități.

Însă cele menționate mai sus nu presupun că nu va avea loc nicio fraudă. Va trebui să implementați anumite practici comerciale, datorită cărora veți putea minimiza riscul de fraudă și pierderile financiare aferente.

Dacă procesați tranzacții CNP, trebuie să fiți mult mai vigilenți. De aceste tranzacții se leagă un risc inerent mai mare, deoarece nu puteți garanta că informațiile vă sunt furnizate de către titularul real al cardului. Prin urmare, acceptarea tranzacțiilor CNP mărește în mod semnificativ vulnerabilitatea dumneavoastră față de fraude, chargeback-uri și în cele din urmă față de pierderi financiare. Aceasta se datorează faptului că nu puteți verifica fizic tranzacția prin realizarea de controale de verificare și prin controlul semnăturii și al PIN-ului titularului de card.

Dacă acceptați tranzacții CNP, nu veți beneficia de aceeași protecție ca un client, care efectuează doar tranzacții în baza contactului personal cu clientul, și dumneavoastră veți fi cei, care vor acoperi chargeback-urile în viitor, în cazul unui litigiu. De asemenea, dacă la o tranzacție CNP apare orice anomalie, o bună practică este realizarea de investigații. Investigațiile pot include atât utilizarea instrumentelor standard pentru zona respectivă de

prevenire a fraudelor, cât și controale pentru verificarea tranzacțiilor din perspectiva „bunului simț".

Nu vă faceți griji cu privire la respingerea comenzilor suspecte. Nu sunteți obligați să realizați o tranzacție, pe care o considerați frauduloasă.

Instrumente de prevenire a fraudelor

Instrumentele de prevenire a fraudelor, precum serviciul de verificare a adreselor (AVS, Address Verification Code) și codul de securitate al cardului (CSC) sunt create pentru a vă ajuta cu autentificarea tranzacției. Spre deosebire de PIN sau semnătură, AVS și CSC nu confirmă identitatea titularului de card, însă dacă sunt folosite concomitent, oferă alte informații, care vă vor ajuta să vă decideți dacă veți realiza tranzacția sau nu.

Codul de securitate al cardului (CSC): CSC oferă alte informații de securitate, al căror obiectiv este de a confirma faptul că clientul are cardul fizic asupra sa. Dacă acest cod este specificat pe card, poate apărea în forma ultimelor trei cifre imprimate pe partea de verso a cardului, pe banda de semnătură, sau în câmpul alb în dreapta benzii de semnătură. La cardurile American Express, acest număr are patru cifre și este imprimat pe partea din față a cardului.

Codul CSC poate fi numit și CVV, CVV2 sau CVC2.

Mastercard SecureCode (SecureCode)/Verified By Visa (VbV): În cazul tranzacțiilor prin Internet, pe site-ul web poate fi implementat un nivel de securitate suplimentar. Soluția SecureCode și VbV, care poate fi descrisă prin denumirea scurtă 3D Secure, a fost dezvoltată pentru a permite clienților să se identifice ca titularii reali ai cardului.

SecureCode și VbV sunt soluții globale pentru tranzacții comerciale pe Internet, care permit titularilor de card să se identifice emitenților de carduri, cu ajutorul unui cod unic personal și a parolei.

Titularul cardului trebuie să introducă parola sa într-o fereastră specială a browser-ului înainte de a putea trece la autorizarea tranzacției online. Emitentul cardului confirmă că cel care realizează tranzacția în momentul respectiv este titularul real. Titularul cardului poate fi liniștit, deoarece știe că nimeni altcineva nu are acces la parola lui, iar dumneavoastră veți obține o dovadă explicită a achiziției autorizate.

În cazul în care în urma unei fraude în cadrul tranzacției online standard trebuie realizat chargeback, comerciantul este obligat să plătească suma contestată a tranzacției. Utilizarea 3D Secure poate transfera această responsabilitate de la comerciant la emitentul cardului. Responsabilitatea este transferată în următoarele condiții:

- comerciantul și operatorul cardului au instalat acest serviciul, însă cardul nu este înregistrat pentru acest serviciu
- comerciantul și titularul cardului s-au înregistrat pentru utilizarea acestui serviciu și titularul cardului se identifică în calitate de titular real
- comerciantul și operatorul cardului au instalat serviciul 3D Secure, însă emitentul cardului nu este autorizat pentru exploatarea acestui serviciu.

Pentru a obține avantajele, pe care le aduce 3D Secure, va trebui să implementați tehnologia solicitată pe site-ul dumneavoastră. Acest lucru poate fi realizat prin încărcarea aplicației înregistrate Merchant Plug-In (MPI) pe serverul dumneavoastră. Eventual puteți încheia un contract cu un prestator de serviciu găzduit, pentru a efectua procesul de autentificare în numele dumneavoastră.

Realizarea tranzacțiilor pe Internet va fi strict pe riscul dumneavoastră, indiferent de faptul dacă cerințele de autorizare sau orice alte cerințe au fost adresate nouă.

Utilizarea procesului de autentificare 3D Secure pentru tranzacțiile pe Internet reduce acest risc. Procesul este disponibil doar pentru cardurile Masercard și Visa. În cazul în care identitatea titularului de card este verificată cu succes prin intermediul SecureCode și/sau VbV, nu poate avea loc chargeback, doar pentru simplul fapt că titularul de card poate respinge realizarea tranzacției. Acest lucru este valabil și atunci când autentificarea este începută, însă nu poate fi finalizată, deoarece titularul de card nu participă la tranzacție cu SecureCode sau VbV, indiferent de motive.

În cazul în care identitatea titularului de card nu poate fi verificată din orice alt motiv, inclusiv defecțiunea dispozitivului dumneavoastră din orice cauză sau orice eroare sau omisiune în cadrul introducerii datelor, pe care ați făcut-o dumneavoastră sau titularul de card, nu veți beneficia de protecția menționată față de chargeback. Procesul de autentificare și impactul acestuia asupra responsabilității pentru tranzacția respectivă acoperă regulile corespunzătoare ale Mastercard și Visa, care se schimbă din când în când. Aceste reguli, printre altele exclud anumite carduri și tranzacții din procesul de autentificare. Aceasta înseamnă că și în cazul în care ați hotărât să utilizați 3D Secure, acest serviciu și protecția pe care o oferă nu se va referi la toate tranzacțiile. Alte informații puteți găsi pe site-ul web Visa și Mastercard. Nu uitați, vă rugăm, că tranzacția poate fi reclamată și vi se poate solicita plata sumei reclamate din orice alt motiv.

Pentru a putea accepta cardurile Maestro prin Internet, trebuie să suportați Mastercard Secure Code. Dacă nu suportați SecureCode pentru tranzacțiile pe Internet cu cardul Maestro, vă expuneți riscului unor sancțiuni financiare semnificative.

Testarea cu scopul depistării fraudelor

Dacă acceptați tranzacțiile CNP, recomandăm cu fermitate să implementați sistemul de testare cu scopul depistării fraudelor, care testează valabilitatea și istoricul cardurilor prezentate pentru realizarea tranzacției.

Printre aceste teste ar trebui să se numere cel puțin controlul de:

- adresă din extras
- țara adresei din extras
- adresă de livrare
- numere de telefon
- tranzacții cu aceeași valoare
- de câte ori a fost folosit cardul în intervalul de timp dat.

De asemenea, în afară de controalele menționate mai sus, recomandăm cu fermitate realizarea următoarelor controale concentrate pe depistarea fraudelor la tranzacțiile pe Internet:

- controlul locației adreselor IP (Internet Protocol) având în vedere țara de emitere a cardului/țara, în care se află adresa de livrare
- verificarea frecvenței de utilizare și a faptului dacă adresele nu sunt conectate cu comenzi de la mai multe adrese de livrare
- Verificarea adreselor de email, care este descrisă în secțiunea de la pag. 46

Zece sfaturi pentru evitarea fraudelor în mediul CNP

Fraudele în mediul CNP pot fi evitate cu vigilență ridicată. În cazul în care angajații de la vânzare pot răspunde la una sau la mai multe din întrebările de mai jos cu „da", nu înseamnă că tranzacția este frauduloasă - dar înseamnă că ar trebui să luați în considerare efectuarea unor alte controale până să finalizați tranzacția.

1. Vânzarea este prea ușoară? Clientul nu manifestă interes față de preț sau detaliile mărfii? Este vorba de un client nou? Adresa clientului se află într-o zonă, în care o acoperă în mod normal activitățile dumneavoastră comerciale? Dacă nu, atunci de ce comandă de la dumneavoastră?
2. Bunurile au o valoare ridicată sau se pot revinde cu ușurință?
3. Suma vânzării este excesiv de ridicată în comparație cu comenzile dumneavoastră obișnuite? Clientul își comandă o cantitate mare de diferite obiecte, sau mai multe bucăți ale aceluiași obiect? Clientul diferă în vreun fel de clienții dumneavoastră obișnuiți?
4. Clientul furnizează datele de pe cardul unei alte persoane, de exemplu al unui client sau membru de familie?
5. Este dispus să vă dea doar numărul de telefon mobil?
6. Adresa arată suspect? Adresa de livrare a mai fost folosită în trecut cu date diferite ale clientului? Adresa de livrare sau de contact se află în străinătate?

Este vorba de un loc public, precum cafenea, stație de benzină, cabană etc.?

7. Clientul solicită livrarea într-un loc neobișnuit într-un anumit interval de timp?

8. Clientul primește instrucțiuni despre ce ar trebui să facă de la o terță persoană, în timp ce vorbește la telefon sau pare a avea rețineri în răspunderea la anumite întrebări?

9. Clientul folosește mai multe carduri pentru a împărți suma totală a cumpărăturilor?

10. Clientul pare a nu cunoaște suficient de bine contul său?

11. Clientul pare a avea probleme în a-și aminti propria adresă de domiciliu și numărul de telefon? Clientul pare a citi din notițe?

ALTE INFORMAȚII IMPORTANTE

VĂ VOM INFORMA PERMANENT

Vă vom transmite în mod regulat actualizări cu privire la chestiuni, care influențează modalitatea în care acceptați și procesați tranzacțiile cu cardurile de credit și de debit.

Este foarte important să citiți aceste actualizări și să vă ghidați după recomandările noastre, îndeosebi acelea, care se referă la modificări obligatorii solicitate de operatorii rețelelor de carduri de plată. Vă rugăm să ne contactați în cazul în care aveți nevoie de ajutor sau sprijin din partea noastră (datele de contact pot fi găsite la pag. 52), sau dacă credeți că nu primiți aceste informații.

ROLELE DE HÂRTIE PENTRU TERMINALELE ELECTRONICE

În cazul în care folosiți un terminal electronic, asigurați-vă că aveți suficiente role de hârtie.

Pentru a comanda role de hârtie, vă rugăm sunați la furnizorul dumneavoastră de produse de birotică, deoarece noi nu oferim role de hârtie partenerilor noștri din rândul comercianților. Asigurați-vă întotdeauna că ați comandat tipul corect pentru terminalul dumneavoastră de plată.

CREAREA PROPRIEI DUMNEAVOASTRE RECLAME

Dacă vreți să creați materiale proprii, în care veți comunica clienților că acceptați carduri de plată ca modalitate de plată, solicitați-ne, vă rugăm, pachetul nostru de materiale vizuale relevante.

Acest pachet oferă informații detaliate despre cum se pot reproduce logourile operatorilor rețelelor de carduri de plată.

Vă rugăm să aveți în vedere că se aplică următoarele reguli:

- logourile cardurilor au fost înregistrate ca mărci înregistrate și trebuie să fie folosite în conformitate cu instrucțiunile cuprinse în pachetul materialelor vizuale
- logourile cardurilor nu pot fi folosite în reclamă într-o manieră, care ar sugera că operatorii rețelelor de carduri de plată promovează serviciile sau bunurile dumneavoastră
- sunteți obligați să ne prezentați spre aprobare toate materialele promoționale sau de vânzare, în care este menționată societatea noastră sau cardurile de orice tip
- pagina dumneavoastră pentru plată pe Internet trebuie să conțină logourile corespunzătoare ale operatorilor rețelelor de carduri de plată.

De asemenea, dacă doriți să folosiți logoul Global Payments pe site-ul dumneavoastră sau în materiale promoționale, trebuie să solicitați acordul scris din partea Global Payments. Vă rugăm să ne contactați în cazul în care doriți să obțineți mai multe informații (datele de contact pot fi găsite la pag. 52).

Fiecare magazin al dumneavoastră trebuie să fie identificat clar în materialul promoțional corespunzător.

CUM NE PUTEȚI CONTACTA

De fiecare dată când ne contactați telefonic, asigurați-vă că aveți pregătit codul dumneavoastră de comerciant. Vă vom căuta în funcție de codul de comerciant, pentru a vă putea identifica. Acest cod este specificat pe factura dumneavoastră lunară și pe chitanțele din terminalele electronice.

Din când în când, apelurile sunt monitorizate și înregistrate în scopul îmbunătățirii serviciilor noastre, pe care vi le oferim. Toate înregistrările rămân exclusiv în proprietatea noastră.

LINIA DE SUPORT GLOBAL PAYMENTS:

+40 373 520 239*
helpdesk@globalpayments.ro

Sau scrieți-ne la:
Global Payments s.r.o., centrála
V Olšinách 626/80
100 00 Praha 10 – Strašnice
Republica Cehă

În România, Global Payments este reprezentat de:
Global Payments s.r.o.
Praga Sucursala București
Calea Victoriei, nr. 15
Sector 3,
România

DACĂ DORIȚI SĂ DEPUNEȚI O PLÂNGERE

Dacă din orice motive nu sunteți mulțumiți în anumite privințe cu serviciile noastre, dorim să luăm cât mai repede legătura cu dumneavoastră. Apoi vom adresa întrebările corespunzătoare și vom încerca să remediem întreaga situație, imediat ce acest lucru va fi posibil.

Vă rugăm apelati la linia noastră de suport și sa ne comunica ti unde a apărut problema. Vom încerca să răspundem imediat plângerii dumneavoastră, iar în cazul în care nu vom putea face acest lucru, vom analiza situația și imediat ce acest lucru va fi posibil, vă vom suna înapoi.

*Telefonul este disponibil de luni până vineri între orele 9am – 5pm, cu excepția sărbătorilor legale. În cazul defectării echipamentului sau pentru probleme legate de tranzacție, vă rugăm să contactați: HELPDESK +40 312 295 455 (disponibil 24/7).

Dacă veți considera că nu am soluționat problema spre mulțumirea dumneavoastră, puteți înainta plângerea dumneavoastră prin intermediul liniei noastre de suport, sau puteți scrie către sediul nostru central, la adresa:

Global Payments s.r.o.
V Olšinách 626/80
100 00 Praga 10 – Strašnice
Republica Cehă
Email: info@globalypayments.cz

Global Payments s.r.o.
Praga Sucursala București
Calea Victoriei, nr. 15
Sector 3,
România

Tel.: +40 373 520 239
Telefonul este disponibil de luni până vineri între orele 9am – 5pm, cu excepția sărbătorilor legale. În cazul defectării echipamentului.

In parteneriat cu

globalpayments

BCR

globalpaymentsinc.com

SERVICE. DRIVEN. COMMERCE

©2017 Global Payments s.r.o.
Toate drepturile sunt rezervate. Toate mărcile înregistrate, denumirile de produse și logourile identificate sau menționate în prezentul document sunt proprietatea posesorilor lor legali.

Global Payments s.r.o., o societate cu răspundere limitată, cu sediul social în V Olšinách 626/80, Strašnice, 100 00 Praga 10, Republica Cehă, având numărul de identificare: 042 35 452, înregistrată în Registrul Comerțului ținut de Curtea Municipală din Praga. Secțiunea C, nr. 244453, acționând în România prin sucursala sa Global Payments s.r.o. Praga Sucursala București, având sediul social în strada Calea Victoriei, nr. 15, Sector 3, București, Romania, înregistrată la Registrul Comerțului București sub nr. J40/12501/2015 și având codul unic de înregistrare (CUI) 35120417.