SMJERNICE ZA PREPOZNAVANJE I SPRJEČAVANJE PRIJEVARA UKRADENIM PODACIMA S PLATNIH KARTICA NA INTERNETSKIM PRODAJNIM MJESTIMA

Kome su namijenjene ove smjernice?

Ove smjernice namijenjene su svim ugovornim partnerima – internetskim prodajnim mjestima.

Tko treba biti upoznat sa sadržajem ovih smjernica?

- odgovorne osobe ugovornih partnera
- svi djelatnici uključeni u procese prodaje, naplate i informatičkog razvoja internetskog prodajnog mjesta
- ostali subjekti koji podržavaju navedene djelatnosti prodajnog mjesta, posebno **davatelji usluga internetskog plaćanja** (*Internet Payment Service Provideri – IPSP*).

Zašto je važno postupanje po navedenim smjernicama?

Pridržavanje svih dolje navedenih smjernica i pravila prilikom prihvaćanja plaćanja platnim karticama obvezno je iz sljedećih razloga:

- **smanjenje broja reklamacija**
- **smanjenje rizika mogućih zloupotreba i posljedične financijske štete**
- **postizanje potrebne sigurnosne, poslovne i regulatorne usklađenosti u kartičnom poslovanju.**

AUTORIZACIJA TRANSAKCIJE

Tehnički pojam autorizacije – odobrenja troška

Tehnička autorizacija transakcije je proces unutar kojeg institucija koja je izdavatelj kartice odobrava ili odbija transakciju određenom karticom u traženom iznosu. Značenje potvrđene autorizacije (odobrenja) jednako je za sve domaće i strane kartice i potvrđuje sljedeće:

1. **broj kartice je ispravan**
2. kartici **nije istekao rok** (Valid thru)
3. kartica **u trenutku autorizacije** nije prijavljena kao **ukradena ili izgubljena**
4. kartica **ima dovoljno** odobrenog **kredita** ili **sredstava** na računu za traženi iznos.

Važno! Tehnička autorizacija transakcije, tzv. odobrenje, važeće je samo ako je suglasnost za transakciju na odgovarajući način dao stvarni korisnik kartice, tj. samo ona osoba čije ime je ispisano na fizičkoj kartici.

Ime i prezime koje kupac unosi na platnim stranicama **nije predmet autorizacije i ne provjerava se automatizmom** kod autorizacije e-commerce transakcija, niti kod kartičnih transakcija općenito.

Autorizacija (odobrenje troška) ne znači potvrdu identiteta stvarnog korisnika i nije jamstvo da transakciju nije moguće naknadno osporiti.

Provođenje transakcije na internetskom prodajnom mjestu

Transakcije na internetskom prodajnom mjestu provode se u dva koraka:

1. Predautorizacija transakcije – Predautorizaciju inicira kupac unosom podataka i potvrdom narudžbe

2. Kompletiranje predautorizacije – Kompletiranje provodi prodajno mjesto u sučelju za pregled i upravljanje transakcijama svog ugovornog davatelja usluge platnog kanala (IPSP-a), nakon provjere transakcije i pripreme robe/usluge za isporuku.

Kompletiranje transakcije potrebno je provesti u roku od 7 dana. Svaka transakcija kompletirana nakon 7 dana može biti osporena od strane korisnika kartica ili banke izdavatelja kartice.

Ako je konačni iznos naplate transakcije **manji od predautoriziranog iznosa**, transakciju je moguće kompletirati na manji iznos.

Svaku predautorizaciju za koju prodajno mjesto zna da je narudžba otkazana ili neće biti poslana na naplatu od strane prodajnog mjesta potrebno je poništiti ("void") u sučelju za upravljanja transakcijama koje osigurava IPSP.

Transakcije za koje predautorizacija nije kompletirana tj. poslana na naplatu, **neće biti poslane** na terećenje kartice **niti plaćene prodajnom mjestu**. Istekom roka važenja predautorizacije istu se više ne može, niti smije slati na naplatu.

Svako prodajno mjesto svakodnevno kontrolira rokove važenja (pred)autorizacija i uspješnost dovršenja predautorizacija kroz elektroničke kanale.

Za ona prodajna mjesta kod kojih se roba/usluga isporučuje odmah, davatelj usluge internetskog platnog kanala može u postavkama prodajnog mjesta zadati da se transakcije iniciraju na način da se (pred)autorizacija i kompletiranje provode u jednom koraku – za takve transakcije nije potrebno dodatno kompletiranje. Iniciranje transakcije u jednom koraku dozvoljeno je isključivo uz suglasnost Nexi Croatia.

NAČELA ODGOVORNOSTI ZA PRIGOVORE I TRANSAKCIJE UKRADENIM PODACIMA O KARTICI

Globalne kartične platne sheme uzele su u obzir prednosti i rizike različitih kanala plaćanja za trgovce, ali i sigurnost i ugodnost kupnje za korisnike koji plaćaju svojim karticama te ustanovile načela odgovornosti i postupanja sudionika kao i pravila o odgovornosti za štetu nastalu u slučajevima osporavanja transakcije:

- neprimitak ili oštećenje robe
- neodgovarajuća kvaliteta robe/usluge u odnosu na opis
- zloupotreba podataka s kartice i druge moguće situacije

Kad je sporna ili prijevarna transakcija provedena na daljinu, **bez prisutnosti kartice**, korištenjem samo podataka s kartice i podataka o korisniku (telefonom, poštom ili putem upisa podataka na internetskom prodajnom mjestu), globalne kartične platne sheme svojim pravilima usmjeravaju odgovornost za financijsku štetu prema instituciji koja za prodajno mjesto obavlja prihvaćanje kartičnog plaćanja odnosno **prema prodajnom mjestu**.

Autentifikacija korisnika kartice

Da bi internetskim prodajnim mjestima pomogle prepoznati i spriječiti sporne transakcije te olakšati upravljanje rizikom štete od zloupotreba, globalne kartične platne sheme su razvile alate autentifikacije korisnika kartice kao i određena međunarodna pravila izuzimanja od financijske odgovornosti (tj. prijenosa) u slučaju prijevarnih transakcija i nastanka štete.

Takvi alati su:

- **AAV za American Express kartice** i
- **3D Secure** (VerifiedByVisa za **VISA** kartice, SecureCode za **Mastercard** kartice).

Ovisno o 3D secure statusu transakcije, definirane su situacije u kojima se **odgovornost za financijsku štetu** od prigovora/zloupotrebe može **'vratiti' odnosno 'prenijeti'** s prodajnog mjesta **na instituciju/banku koja je izdala karticu** – bez obzira što se zloupotreba kartice uistinu dogodila na internetskom prodajnom mjestu.

*Od Vašeg davatelja usluge internetskog sustava za plaćanje (Internet Payment Service Provider) zatražite informaciju i uputu o tome **gdje u sustavu koji Vi koristite vidite podatak o statusu AAV provjere i status 3D Secure provjere** za svaku transakciju.

AAV (*"Automated Address Verification"*) Automatska verifikacija adrese

American Express kartice trenutno nisu uključene u 3D Secure sustav provjere, a kao dodatni alat u kontroli prijevarnih transakcija, American Express i Nexi Croatia osiguravaju AAV servis – automatsku verifikaciju adrese.

Tablica rezultata AAV provjere za transakcije American Express karticama*	
Odgovor	Opis odgovora
Y	Upisani podaci o adresi i poštanskom broju su ispravni – AAV provjera je ispravna
A	Upisani podatak o adresi je ispravan, podatak o poštanskom broju je neispravan – AAV provjera djelomično ispravna
Z	Upisani podatak o poštanskom broju je ispravan, upisani podatak o adresi je neispravan – AAV provjera djelomično ispravna
N	Upisani podaci o adresi i poštanskom broju su neispravni
U, S, R ili prazno polje	AAV usluga provjere nije podržana ili je trenutno nedostupna – izdavatelj kartice ili unesena kartica ne podržavaju AAV uslugu provjere

* Rezultati AAV provjere nisu sistemski parametar za automatsko odobrenje ili odbijanje autorizacije, niti su potvrda identiteta stvarnog korisnika kartice, već služe kao dodatna provjera za prodajna mjesta u smislu ispravnosti unesene adrese računa prilikom obavljanja internetske kupnje – prodajno mjesto samo donosi konačnu odluku o završetku procesa autorizacije (naplati) ili otkazivanju transakcije.

3D Secure (VerifiedByVisa, MC SecureCode)

3D Secure protokol autentifikacije kartice ima za cilj povećati stupanj zaštite internetskih prodajnih mjesta u slučaju prijevarnih transakcija ili neopravdanih prigovora kupaca, ali ne isključuje od odgovornosti za moguću štetu bezuvjetno, nego prema propisanim pravilima kartičnih mreža Mastercard i VISA.

Tablica u nastavku je općeniti prikaz tri osnovne situacije, od kojih **u dvije situacije može doći do prijenosa odgovornosti** s prodajnog mjesta **na izdavatelja kartice**.

Pregled osnovnih situacija u 3D secure okruženju autentifikacije i prijenos odgovornosti u slučaju zloupotrebe					
Situacija	**Visa** ECI flag*	**Mastercard** UCAF flag*	Status	Objašnjenje	ODGOVORNOST ZA FINANCIJSKU ŠTETU
1	5	2	**Secured** – provjera uspješna	3D Secure provjera kupca uspješno provedena	Odgovornost se prenosi na **IZDAVATELJA/ KORISNIKA KARTICE** koja je korištena u zloupotrebi
2	6	1	**Attempted** – provjera pokušana	Pokušana je 3D Secure provjera, ali nije provedena, jer kartica kupca ili izdavatelj kartice nije u 3D Secure programu.	Odgovornost se prenosi na **IZDAVATELJA KARTICE**, ali iznimno***, odgovornost u slučaju zloupotrebe može u pojedinim slučajevima*** ostati na prodajnom mjestu
3	7	0	**Unsecured** – provjera nije moguća	3D secure provjeru nije moguće provesti, prodajno mjesto provodi dodatnu provjeru prema internoj proceduri provjere	ODGOVORNOST OSTAJE NA PRODAJNOM MJESTU U slučaju zloupotrebe, odgovornost za transakciju ostaje na prodajnom mjestu na kojem je provedena transakcija, a dodatne kontrole **propisuje i provodi PRODAJNO MJESTO****

** U slučaju neuspješne provjere (situacija 3) ili u slučaju da je potvrđeno da kartica nije uključena u 3D Secure program (situacija 2) preporučuje se oprez i dodatna provjera podataka o kupcu i narudžbi prema indikatorima sumnjivih transakcija odnosno prema internim politikama.

*** Mastercard i VISA pod određenim uvjetima i za neke proizvode (npr. tzv. komercijalne kartice, prepaid kartice) propisuju pravila prema kojima je prijenos odgovornosti na izdavatelja kartice isključen bez obzira na navedene statuse u situaciji 2 ili 3 – tehnički nije moguće prikazati sve transakcijske parametre prema kojima bi se u trenutku provođenja autorizacije moglo znati radi li se o ovakvom izuzetku - prodajno mjesto samo određuje koje dodatne provjere želi provesti radi točnog utvrđivanja identiteta korisnika kartice.

MJERE OPREZA – SPRJEČAVANJE PRIJEVARA, PROVJERAVANJE IDENTITETA

Bez obzira na rezultate AAV provjere ili 3D secure statusa transakcije, provjeravajte sve transakcije – posebno one kod kojih postoje pokazatelji za moguće osporavanje ili zloupotrebu kartice. Takvi mogući pokazatelji rizičnosti transakcije su najčešće:

- **više** različitih **transakcija** ili **odbijenih** transakcija **različitim karticama**, pogotovo uz navedeno **isto ime kupca** ili **istu adresu**, **broj telefona** ili **e-mail adresu**, **IP adresu**
- **različito ime i prezime korisnika kartice** (posebno ako je navedeno strano ime) i **ime osobe za primitak robe** odnosno kontakt (ovisno o tome koji od navedenih podataka su dostupni djelatnicima internetskog prodajnog mjesta kod narudžbe – ovisno o vrsti prodajnog mjesta s Vašim IPSP-om, osigurajte obvezan uvid u sve podatke koji su potrebni za procjenu rizičnosti transakcije)
- transakcije se obavljaju **karticama STRANE banke/izdavatelja izvan Hrvatske**, pogotovo izvan Europe*
- iznosi transakcija su **viši od uobičajenih** ili **neobično visoki za vaš tip prodajnog mjesta** (plaća se skupa ili lako utrživa roba/usluga)
- **kupac požuruje isporuku**, uporan je, traži isporuku žurno ili **želi preuzeti robu osobno** u prostorijama trgovca, a **pri tome nema karticu** kojom je plaćeno kod sebe, uz razne izgovore već postoje i gore spomenuti indikatori
- rezervacija ili traženje ponude natprosječno skupih roba/usluga/aranžmana, **dodatne unutarnje i vanjske usluge** (express dostave, vanjski suradnici i sl.), posebice na **adrese na otvorenim prostorima** i **u inozemstvo** (npr. hitno, za VIP goste i sl.)
- naručitelj inicira **transakcije s više različitih kartica** za plaćanje odmah ili nakon odbijene autorizacije
- kupac plaća usluge unaprijed i **naknadno otkazuje** rezervaciju/kupnju, pa potom traži POVRAT DIJELA IZNOSA, u pravilu drugim kanalom, a ne na karticu/e s kojih su uplate obavljene – česti su izgovori kupca poput obiteljskih nesreća, automobila, kuća ili kartica koje su izgorjele u požaru

Ako postoji sumnja u istinitost podataka o stvarnom korisniku kartice, prodajno mjesto može:

- poduzeti dodatne provjere prije realizacije usluge
- promijeniti e-commerce kanal naplate u onaj koji pruža veću razinu tehničke i ugovorne zaštite za prodajno mjesto (npr. preusmjeravanje naplate na prodajno mjesto i očitavanje čipa fizičke kartice umjesto e-commerce transakcije)
- zatražiti dodatnu provjeru od Nexi Croatia na monitoring@nexigroup.com
- odustati od isporuke robe za rizičnu transakciju i o tome obavijestiti Nexi Croatia.

* Od Vašeg davatelja usluge internetskog sustava za plaćanje (Internet Payment Service Provider) zatražite informaciju i uputu o tome **kako u sustavu koji Vi koristite možete prepoznati i pratiti**:

- transakcije koje su obavljene **stranim karticama**
- odbijene, ne samo odobrene transakcije
- **korištenje različitih kartica** od strane i**stog korisnika**, s istom adresom isporuke ili e-mail adresom ili istim brojem telefona za kontakt.

OBVEZNA ZAŠTITA PODATAKA I PRIMJENA PCI DSS STANDARDA

Sva prodajna mjesta, posebice internetska, moraju poštivati pravila PCI DSS standarda zaštite podataka o karticama.

- zatražite od vašeg IPSP-a uputu kako provesti postupak PCI DSS certifikacije za vaše prodajno mjesto
- dokaz o provođenju potrebne razine certifikacije dostavite prihvatitelju svake godine
- od svakog davatelja usluge/servisa vezanih uz vaše internetsko prodajno mjesto zatražite da vam da dokaz da je proizvod/usluga koju vam pruža u skladu s PCI DSS standardom.
  Ovo se posebno odnosi na:
  - IPSP, sustave zaprimanja rezervacija/narudžbi
  - servise za hosting web stranica ili poslovnih sustava
  - cloud servise
  - web programiranje
  - održavanje informacijskih sustava tvrtke
  - internet mail ili
  - fax servise
- svedite na najmanju mjeru čuvanje bilo kakvih podataka o karticama. Budite sigurni da svi davatelji pratećih usluga vašem poslovanju imaju odgovarajući nivo PCI DSS certifikata izdanog od strane ovlaštenog certifikatora.

Internetska prodajna mjesta obvezna su svake godine dostaviti pisani dokaz usklađenosti s PCI DSS standardom.

U svim načinima čuvanja ili komunikacije prema korisniku kartice (kad broj nije potreban za samo iniciranje transakcije) **puni broj kartice i rok važenja moraju biti prikriveni** (osim 4 zadnje znamenke broja kartice). Detaljnije obveze prema kategoriji Vašeg prodajnog mjesta provjerite na **https://www.pcisecuritystandards.org**

Prodajna mjesta ne smiju na bilo koji način **čuvati niti tražiti dostavu kontrolnog broja kartice.**

Nexi Croatia **ne dozvoljava** unošenje kontrolnog broja od strane prodajnog mjesta, već isključivo od strane korisnika kartice i isključivo u sučelju internetske platne stranice sa sigurnim elektroničkim kanalom (najmanje TLS 1.2 enkripcija).

STALNA EDUKACIJA NOVIH I POSTOJEĆIH DJELATNIKA I RUKOVODITELJA

Prodajna mjesta dužna su kontinuirano provoditi edukaciju djelatnika i odgovornih osoba uključenih u procese vezane za prihvaćanje plaćanja karticama. Navedeno se odnosi na poznavanje potrebnih pravila i smjernica za kartično plaćanje te osiguranje da su potrebne smjernice, upute i informacije dostupne djelatnicima prema njihovoj ulozi u ovom procesu. Akcije edukacije potrebno je provoditi uvijek prije očekivanih pojačanih aktivnosti naplate kao što su sezonska/blagdanska povećanja prometa, akcijske ponude, uvođenje novih ili atraktivnih proizvoda i sl.

Za više informacija o edukaciji djelatnika, rukovoditelja i odgovornih osoba prodajnih mjesta kontaktirajte Nexi Croatia.

KONTAKTI

Autorizacije transakcija:
tel.: +385 1 612 44 00
e-mail: autorizacije@pbzcard.hr

Poslovni uvjeti i ugovaranje prihvaćanja:
tel.: +385 1 612 44 99
e-mail: prodaja@pbzcard.hr

Tim za tehničku podršku prodaji:
tel.: +385 1 612 42 77
e-mail: info.prodajnamjesta@nexigroup.com

Praćenje transakcija i prevencija zloupotreba:
tel.: +385 1 612 42 42
e-mail: monitoring@pbzcard.hr

Nexi Croatia d.o.o.
Radnička cesta 50, 10000 Zagreb
www.nexi.hr

Ožujak 2023.