

Radni pravilnik za sigurnost podataka (DSOP)

Odjeljak 1	Uvod u DSOP i Standarde za zaštitu	3
Odjeljak 2	PCI DSS program sukladnosti (Važna periodična provjera valjanosti Vaših sustava)	3
Korak 1:	Sudjelovanje u Programu sukladnosti tvrtke American Express u okviru ovog Pravilnika	4
Korak 2:	Razumijevanje Vašeg zahtjeva u vezi Dokumentacije za provjeru valjanosti Razine Trgovca/Davatelja usluge	4
Korak 3:	Ispunjavanje Dokumentacije za provjeru valjanosti koju morate poslati tvrtki American Express	7
Korak 4:	Slanje Dokumentacije za provjeru valjanosti tvrtki American Express	9
Odjeljak 3	Obveze za upravljanje Podatkovnim incidentima	10
Odjeljak 4	Obveze obeštećenja zbog Podatkovnog incidenta	12
Odjeljak 5	Program ciljane analize (TAP)	14
Odjeljak 6	Povjerljivost	15
Odjeljak 7	Odricanje od odgovornosti	16
Odjeljak 8	Pojmovnik	16
Odjeljak 9	Korisna web-mjesta	20

DSOP Sažetak izmjena

Ikone

Važna ažuriranja su data u popisu u Tablici sa sažetkom izmjena, a naznačena su i u *DSOP-u* s trakom promjena. Traka promjena je okomita crta, obično se nalazi na lijevoj margini koja označava dodani ili promijenjeni tekst. Samo značajne promjene u *DSOP-u* potencijalnim utjecajem na radne postupke Trgovca kako je prikazano na lijevoj margini.



Uklonjeni tekst označen je ikonom kante za smeće koja se nalazi u margini pored brisanja značajnog teksta, uključujući odjeljke, tablice, odlomke, napomene i točke nabiranja. Uklonjeni tekst navodi se u Sažetku izmjena uz pomoć numeriranja teksta iz prethodnog izdanja kako bi se izbjegla zbrka.

Odlomci uokvireni plavim crtama označavaju informacije za određenu regiju.

Tablica sa sažetkom izmjena

Važna su ažuriranja navedena u sljedećoj tablici i također su naznačena u *DSOP-u* s trakom promjena.

Odjeljak/Pododjeljak	Opis izmjene
Nema promjena za ovo izdanje.	

Odjeljak 1 Uvod u DSOP i Standarde za zaštitu

Kao lider u zaštiti potrošača, tvrtka American Express oduvijek se zalaže za zaštitu Podataka vlasnika kartice i Osjetljivih podataka za provjeru autentičnosti te osiguravanje njihove zaštite.

Kompromitiranje podataka negativno utječe na potrošače, Trgovce, Davatelje usluga, i izdavatelje kartica. Čak i samo jedan incident može značajno naštetiti reputaciji tvrtke i pogoršati njezinu mogućnost učinkovitog poslovanja. Hvatanje u koštac s tom prijetnjom i uvođenje radnih pravilnika za sigurnost mogu pridonijeti poboljšanju povjerenja stranaka, povećanju profitabilnosti i reputacije tvrtke.

Tvrtka American Express zna da naši Trgovci i Davatelji usluga (zajedno, Vi) dijele našu zabrinutost i zahtijeva da, kao dio naših odgovornosti, Vi budete u skladu s odredbama za sigurnost podataka u vašem Ugovoru za prihvaćanje (u slučaju Trgovaca) ili obradu (u slučaju Davatelja usluga) Kartice American Express® (svaki se naziva **Ugovor**) te ovog Radnog pravilnika za sigurnost podataka (DSOP), koji možemo promijeniti s vremena na vrijeme. Ti se zahtjevi odnose na svu Vašu opremu, sustave i mreže (i njihove komponente) putem koje se Ključevi za šifriranje, Podaci vlasnika kartice ili Osjetljivi podaci za provjeru autentičnosti (ili njihova kombinacija) spremaju, obrađuju ili prenose.

Značenje izraza u navodnicima koji ovdje nisu definirani navode se u pojmovniku na kraju ovog pravilnika.

Radni pravilnik za sigurnost podataka (DSOP) skup je opsežnih zahtjeva za pravila predviđenih za zaštitu Podataka računa kad god se podaci pohranjuju, obrađuju ili prenose.

American Express traži da svi Trgovci i Davatelji usluge budu sukladni Standardu za sigurnost podataka u industriji platnih kartica (PCI DSS). O okviru tog zahtjeva, Vi morate, a morate navesti i Vaše Obuhvaćene stranke na sljedeće:

- spremati Podatke vlasnika kartice samo za vršenje Transakcija putem Kartice American Express u skladu s Ugovorom i kako je zahtijevano njime.
- djelovati sukladno s trenutnim PCI DSS-om i drugim Zahtjevima PCI Security Standards Council (PCI-SSC) koji se mogu primijeniti na obradu, spremanje ili prijenos Ključeva za šifriranje, Podataka vlasnika kartica ili Osjetljivih podataka za provjeru autentičnosti ne kasnije od datuma stupanja na snagu za uvođenje te inačice važećeg zahtjeva.
- paziti da koristite PCI odobrene proizvode pri uporabi ili zamjeni tehnologije za pohranu, obradu ili prijenos podataka.

Morate zaštititi sve zapise o Naplati American Express i zadržane Kreditne zapise u skladu s Ugovorom te u skladu s ovim odredbama za sigurnost podataka; te zapise smijete koristiti samo za svrhe Ugovora i morate ih čuvati na primjeren način. Financijski i na drugi način odgovarate tvrtki American Express za osiguravanje sukladnosti svojih Obuhvaćenih stranaka s ovim odredbama za sigurnost podataka (umjesto iskazivanja sukladnosti vaših Obuhvaćenih stranaka s ovim pravilnikom u okviru [Odjeljak 2, „PCI DSS program sukladnosti \(Važna periodična provjera valjanosti Vaših sustava\)“](#), osim ako se u tom odjeljku ne navodi drugačije). Podaci koji se odnose na PCI standarde i način ostvarivanja sukladnosti njihovim zahtjevima mogu se pronaći na www.pcisecuritystandards.org.

Odjeljak 2 PCI DSS program sukladnosti (Važna periodična provjera valjanosti Vaših sustava)

Trebate izvršiti sljedeće korake godišnje i svakih 90 dana kako biste u okviru PCI DSS-a na način opisan u nastavku provjerili valjanost statusa opreme Vaših primatelja Franšize, sustava i/ili mreže (i njihovih komponenti) na kojima se spremaju, obrađuju ili prenose Podaci Vlasnika kartica ili Osjetljivi podaci za provjeru autentičnosti.

Za dovršenje provjere valjanosti potrebna su četiri koraka:

- [Korak 1:](#) Sudjelovanje u Programu sukladnosti tvrtke American Express s PCI-em u okviru ovog pravilnika.
- [Korak 2:](#) Razumijevanje Vašeg zahtjeva u vezi Dokumentacije za provjeru valjanosti Razine Trgovca/Davatelja usluge.
- [Korak 3:](#) Ispunjavanje Dokumentacije za provjeru valjanosti koju morate poslati tvrtki American Express.

- [Korak 4:](#) Slanje Dokumentacije za provjeru valjanosti tvrtki American Express u zadanom roku.

Korak 1: Sudjelovanje u Programu sukladnosti tvrtke American Express u okviru ovog Pravilnika

Trgovci razina 1 i 2 te svi Davatelji usluga, kako je opisano u nastavku, moraju sudjelovati u Programu u okviru ovog pravilnika. American Express može po vlastitom nahođenju odrediti da neki Trgovci razina 3 i 4 moraju sudjelovati u Programu u okviru ovog pravilnika.

Trgovci i Davatelji usluga koji moraju sudjelovati u Programu moraju se prijaviti na [Portal](#) koji omogućuje administrator Programa kojeg odabere American Express u zadanom roku.

- Morate prihvatiti sve razumne uvjete i odredbe za upotrebu Portala.
- Morate odrediti najmanje jedan kontakt za sigurnost podataka na Portalu te navesti njegove točne podatke. Potrebni podaci sadrže:
 - Ime i prezime
 - Adresa e-pošte
 - Broj telefona
 - Fizička poštanska adresa
- Morate navesti ažurirane ili nove podatke za kontakt osobe za sigurnost podataka na Portalu ako se ti podaci promijene.
- Morate provjeriti jesu li Vaši sustavi ažurirani kako bi bilo moguće slanje poruka s domene Portala.

Ako ne navedete valjane podatke za kontakt ili ih ne održavate ili ne omogućite slanje e-pošte, to neće utjecati na naša prava na procjenu naknade.

Korak 2: Razumijevanje Vašeg zahtjeva u vezi Dokumentacije za provjeru valjanosti Razine Trgovca/Davatelja usluge

S obzirom na količinu Transakcija putem Kartica American Express, postoje četiri Razine Trgovca i dvije Razine Davatelja usluge.

- Za trgovce to je volumen prometa koji dostavljaju njihove Organizacije koji doseže najvišu razinu računa trgovca za American Express.*
- Za Davatelje usluga to je ukupna količina koji dostavljaju Davatelji usluga i Davatelji usluga subjekata kojima pružate usluge.

Platne transakcije koje pokreće kupac (Buyer Initiated Payments, BIP) nisu uključene u količinu Transakcija putem Kartica American Express za utvrđivanje Razine Trgovca i zahtjeva za provjeru valjanosti. Svrstavate se u jednu od Razina Trgovca navedenih u [Tablica A-1: Razina Trgovca i Davatelja usluga](#).

* To u slučaju Davatelja franšize uključuje količinu iz jedinica u njihovoj Franšizi. Franšizodavci koji svojim Primateljima franšize nalažu primjenu specificiranog Sustava točke prodaje (Point of Sale, POS) ili Davatelji usluga također moraju dostaviti dokumentaciju za provjeru valjanosti za zahvaćene primatelje franšize.

Tablica A-1: Razina Trgovca i Davatelja usluga

Razina Trgovca	Broj American Express Transakcija godišnje
Trgovac razine 1	2,5 milijuna ili više Transakcija putem Kartice American Express godišnje ili Trgovac kojeg tvrtka American Express svojom odlukom svrsta u Razine 1.
Trgovac razine 2	od 50.000 do manje od 2,5 milijuna Transakcija putem Kartice American Express godišnje.
Trgovac razine 3	od 10.000 do manje od 50.000 Transakcija putem Kartice American Express godišnje.
Trgovac razine 4	manje od 10.000 Transakcija putem Kartice American Express godišnje.
Razina Davatelja usluga	Broj American Express Transakcija godišnje
Davatelj usluge razine 1	2,5 milijuna ili više Transakcija putem Kartice American Express na godinu ili Davatelj usluga kojeg tvrtka American Express inače smatra Davateljem usluge Razine 1.
Davatelj usluge razine 2	manje od 2,5 milijuna Transakcija putem Kartice American Express na godinu ili svi Davatelji usluga koje tvrtka American Express ne smatra Davateljima usluge Razine 1.

Zahtjevi za Dokumentaciju za provjeru valjanosti za Trgovca

Trgovci (ne i Davatelji usluga) mogu se klasificirati u četiri Razine Trgovca. Nakon utvrđivanja Razine Trgovca iz [Tablica A-1: Razina Trgovca i Davatelja usluga](#) (gore), pogledajte [Tablica A-2: Dokumentacija za provjeru valjanosti Trgovca](#) kako biste utvrdili zahtjeve za dokumentaciju za provjeru valjanosti.

Tablica A-2: Dokumentacija za provjeru valjanosti Trgovca

Razina Trgovca/ broj American Express Transakcija godišnje	Izvešće o sukladnosti Potvrda o sukladnosti (ROC AOC)	Upitnik za samoprocjenu sukladnosti (SAQ AOC) I 90- dnevno skeniranje ranjivosti vanjske mreže (skeniranje)	Program za unaprjeđenje sigurnosne tehnologije (STEP) Potvrda programa za prikladne Trgovce
Razina 1/ 2,5 milijuna ili više	Obvezno	Nije primjenjivo	Neobvezno uz odobrenje tvrtke American Express (zamjenjuje ROC)
Razina 2/ 50.000 do manje od 2,5 milijuna	Opcija	SAQ AOC obvezan (osim ako se dostavlja ROC AOC); skeniranje obvezno za određene kategorije SAQ-a	Neobvezno uz odobrenje tvrtke American Express* (zamjenjuje SAQ i skeniranje mreže ili ROC)
Razina 3**/ 10.000 do manje od 50.000	Opcija	SAQ AOC je opcija (obvezan ako to traži American Express); skeniranje obvezno s određenim kategorijama SAQ-a	Neobvezno uz odobrenje tvrtke American Express* (zamjenjuje SAQ i skeniranje mreže ili ROC)
Razina 4**/ manje od 10.000	Opcija	SAQ AOC je opcija (obvezan ako to traži American Express); skeniranje obvezno s određenim kategorijama SAQ-a	Neobvezno uz odobrenje tvrtke American Express* (zamjenjuje SAQ i skeniranje mreže ili ROC)

* **Napomena:** American Express PCI tim će pregledati zahtjev i ocijeniti prikladnost te potvrditi ako se kvalificirate za STEP Program. Molimo da kontaktirate svog upravitelja strankama i/ili da se obratite na AXPPCIComplianceProgram@aexp.com da provjerite prikladnost.

**Radi otklanjanja sumnje, Trgovci razina 3 i 4 ne trebaju dostavljati Dokumentaciju za provjeru valjanosti ako to ne zatraži tvrtka American Express po vlastitom nahođenju, ali svakako moraju biti sukladni i odgovorni u pogledu svih drugih odredbi ovog Radnog pravilnika za sigurnost podataka.

American Express zadržava pravo da provjeri cjelovitost, točnost i prikladnost Vaše dokumentacija za provjeru valjanosti PCI-a. American Express može tražiti da pošaljete dodatne dokumente za procjenu u ovu svrhu. Pored toga, American Express ima pravo od Vas tražiti da angažirate Kvalificiranog procjenitelja sigurnosti (QSA) s odobrenjem od PCI Security Standards Council ili PCI Forenzičkog istražitelja (PFI).

Zahtjevi u vezi Dokumentacije za provjeru valjanosti Davatelja usluge

Davatelji usluga (ne Trgovci) mogu se klasificirati u dvije Razine. Nakon utvrđivanja Razine Davatelja usluge iz [Tablica A-1: Razina Trgovca i Davatelja usluga](#) (gore), pogledajte [Tablica A-3: Dokumentacija za provjeru valjanosti Davatelja usluge](#) kako biste utvrdili zahtjeve za dokumentaciju za provjeru valjanosti.

Davatelji usluge ne zadovoljavaju uvjete za STEP.

Tablica A-3: Dokumentacija za provjeru valjanosti Davatelja usluge

Razina	Dokumentacija za provjeru valjanosti	Zahtjev
1	Godišnje izvješće o sukladnosti – Potvrda o sukladnosti (ROC AOC)	Obvezno
2	Godišnji SAQ D (Davatelj usluga) ili 90-dnevno skeniranje mreže ili Godišnje izvješće o sukladnosti – Potvrda sukladnosti (ROC AOC), u skladu sa željama	Obvezno

Preporučuje se da Davatelji usluge budu u skladu i s PCI dodatnom provjerom valjanosti za namjenske subjekte.

Program za unaprjeđenje sigurnosne tehnologije (STEP)

Trgovci koji su sukladni s PCI DSS-om mogu, ako American Express tako odluči, ispunjavati i uvjete STEP-a tvrtke American Express ako koriste određene dodatne sigurnosne tehnologije u svojim okruženjima za obradu Kartica. Program STEP primjenjuje se samo ako se Trgovcu nije dogodio Podatkovni incident tijekom proteklih 12 mjeseci i ako se 75% svih Kartičnih Transakcija Trgovca vrši uz kombinaciju sljedećih naprednih opcija za sigurnost:

- **EMV, beskontaktni ili digitalni novčanik** – na aktivnom uređaju koji podržava čipove s valjanim i važećim odobrenjem/certifikatom EMVCo (www.emvco.com) odobrenjem/certifikatom i koji može obrađivati Transakcije karticama s čipom sukladno s AEIPS-om. (Za trgovce u SAD-u moraju se uključiti Beskontaktna transakcije)
- **Šifriranje od točke do točke (Point-to-Point Encryption, P2PE)** – komuniciranje s procesorom trgovca putem PCI-SSC ili QSA odobrenog Sustava šifriranja od točke do točke
- **Tokenizirano** – rješenje za tokenizaciju mora:
 - ispunjavati specifikacije za EMVCo
 - biti zaštićeno, obrađeno, pohranjeno, preneseno i u potpunosti pod upravljanjem davatelja usluge treće strane sukladnom s PCI-em
 - Trgovac ne smije vidjeti Stalne broje računa (PAN) na tokenu.

Trgovci koji zadovoljavaju uvjete za STEP imaju smanjene potrebe za PCI dokumentaciju za provjeru valjanosti, kao što je dodatno opisano u [Korak 3: „Ispunjavanje Dokumentacije za provjeru valjanosti koju morate poslati tvrtki American Express“](#) u nastavku.

Korak 3: Ispunjavanje Dokumentacije za provjeru valjanosti koju morate poslati tvrtki American Express

Sljedeći dokumenti potrebni su za različite razine Trgovaca i Davatelja usluge, kako je navedeno u [Tablica A-2: Dokumentacija za provjeru valjanosti Trgovca](#) i [Tablica A-3: Dokumentacija za provjeru valjanosti Davatelja usluge](#) iznad.

Morate dostaviti Potvrdu o sukladnosti (AOC) za odgovarajuću vrstu procjene. AOC je potvrda Vašeg statusa sukladnosti i kao takvu mora je potpisati i datirati osoba odgovarajuće razine rukovodstva Vaše organizacije.

Osim AOC-a, American Express može tražiti da dostavite presliku cijele procjene i po vlastitom nahođenju, dodatnih dokumenata koji pokazuju sukladnost sa zahtjevima PCI DSS-a. Takvu Dokumentaciju za provjeru valjanosti nabavljate o svom trošku.

Izvjешće o sukladnosti – Ovjera sukladnosti (ROC AOC) - (godišnja obveza) – Izvjешće o sukladnosti prikazuje rezultate detaljne procjene na lokaciji opreme, sustava i mreža (i njihovih komponenti) u kojima se pohranjuju,

obrađuju ili prenose Podaci vlasnika kartice ili Osjetljivi podaci za provjeru autentičnosti (ili oboje). Postoje dvije verzije: jedna za Trgovce, a druga za Davatelje usluga. Izvješće o sukladnosti mora sastaviti:

- QSA ili
- Interni procjenitelj sigurnosti (ISA) ga morate Vi sastaviti uz ovjeru Vašeg glavnog izvršnog direktora, glavnog financijskog direktora, izvršnog direktora za sigurnost informacijskih sustava ili glavnog direktora

ROC AOC mora potpisati i datirati QSA ili ISA te Osoba odobrene razine rukovodstva Vaše organizacije nakon čega se dostavlja tvrtki American Express najmanje jednom godišnje.

Godišnji upitnik za samoprocjenu sukladnosti (SAQ AOC) - (godišnja obveza) – Upitnik za samoprocjenu sukladnosti omogućuje vam da ispitete svoju opremu, sustave i mreže (i njihove komponente) u kojima se pohranjuju, obrađuju ili prenose Podaci vlasnika kartice ili Osjetljivi podaci za provjeru autentičnosti (ili oboje). Postoji više verzija SAQ-a. Trebate odabrati jednu ovisno o Podatkovnom okruženju vlasnika kartice.

SAQ može ispuniti osoblje Vaše Tvrtke kvalificirano za davanje točnih i temeljitih odgovora na pitanja, a možete i zaposliti QSA-a kao ispomoć. SAQ AOC mora potpisati i datirati osoba s odobrene razine rukovodstva Vaše organizacije nakon čega se dostavlja tvrtki American Express najmanje jednom godišnje.

Sažetak skeniranja ranjivosti vanjske mreže od odobrenog Davatelja usluga skeniranja (skeniranje ASV-a) - (obveza slanja svakih 90 dana) – skeniranje vanjskih ranjivosti test je koji se provodi na daljinu za utvrđivanje mogućih slabosti, ranjivosti i pogrešnih konfiguracija komponenti Podatkovnog okruženja vlasnika kartice koje se povezuju na internet (kao što su mrežne stranice, aplikacije, mrežni poslužitelji, poslužitelji za e-poštu, javne domene ili hostovi).

Skeniranje ASV-a treba izvršiti Odobreni davatelj usluga skeniranja (Approved Scanning Vendor, ASV).

Ako to zahtijeva SAQ, morate dostaviti izvješće ASV-a o skeniranju za Potvrdu o sukladnosti skeniranja (AOSC) ili izvršni sažetak s brojem skeniranih ciljeva, potvrdu da rezultati ispunjavaju procedure skeniranja PCI DSS-a te status sukladnosti koji ispunjava ASV tvrtki American Express najmanje svakih 90 dana.

Ako podnosite ROC AOC ili STEP nisu potrebni za dostavu Izvršnog sažetka AOSC-a ili skeniranja ASV-a osim ako je tako posebno zatraženo. Kako bi se izbjegle nedoumice, Skeniranje je obvezno ako je to zahtjev primjenjivog upitnika SAQ.

Dokumentacija za provjeru valjanosti ovjere programa (STEP) - (godišnja obveza) – STEP je dostupan samo za trgovce koji ispunjavaju kriterije navedene u [Korak 2: „Razumijevanje Vašeg zahtjeva u vezi Dokumentacije za provjeru valjanosti Razine Trgovca/Davatelja usluge“](#) gore. Ako Vaša tvrtka ispunjava te uvjete, morate ispuniti i poslati obrazac ovjere programa STEP tvrtki American Express jednom godišnje. Predložak obrasca za godišnju ovjeru programa STEP dostupan je za preuzimanje na [Portal](#)u. Također se možete obratiti Vašem Upravitelju za stranke ili pisati u American Express na AXPPCComplianceProgram@aexp.com.

Nesukladnost s PCI DSS - (godišnja, tromjesečna i ad hoc obveza) – Ako niste sukladni a PCI DSS, tada morate poslati PCI Sažetak alata za utvrđivanje prioriteta (PAT) (dostupan za preuzimanje s mrežne stranice PCI Security Standards Council).

PAT Sažetak mora biti utvrditi rok za otklanjanje problema, koji, ako se želi postići sukladnost, ne smije biti duži od dvanaest (12) mjeseci od sastavljanja dokumenata. Tvrtku American Express morate povremeno obavještavati o napretku u otklanjanju Statusa nesukladnosti (Trgovci razina 1, 2, 3 i 4, svi Davatelji usluga). Koraci za otklanjanje nesukladnosti s PCI DSS-om vrše se o Vašem trošku.

Tvrtka American Express neće naplaćivati naknadu za nesukladnost prije datuma za otklanjanje problema. Prema [Tablica A-4: Naknada za nesukladnost](#), i dalje ćete biti odgovorni tvrtki American Express u pogledu svih obveza za obeštećenjem za podatkovni incident i morat ćete poštivati sve druge odredbe iz ovog pravilnika.

American Express ima prema vlastitom nahođenju zadržava pravo nametanja naknada za nesukladnost ako:

- nije poslan PCI Obrazac za utvrđivanje prioriteta u skladu sa zahtjevima navedenim u ovom odjeljku,
- nisu ispunjeni koraci za obeštećenje zacrtani u PCI Obrascu za utvrđivanje prioriteta za Status nesukladnosti,
- nije ispunjen bilo koji zahtjev u PCI Obrascu za utvrđivanje prioriteta za Status nesukladnosti ili

- obvezna dokumentacija o sukladnosti nije dostavljana u American Express do zadanog roka ili nakon zahtjeva.

Trgovci/Davatelji usluge koji nisu sukladni zahtjevima detaljno opisanima u [Korak 2: „Razumijevanje Vašeg zahtjeva u vezi Dokumentacije za provjeru valjanosti Razine Trgovca/Davatelja usluge“](#), možda podliježe naknadama kako je navedeno u [Korak 4: „Slanje Dokumentacije za provjeru valjanosti tvrtki American Express“](#).

Radi otklanjanja svake sumnje, Trgovci koji nisu sukladni s PCI DSS-om ne ispunjavaju uvjete za STEP.

Korak 4: Slanje Dokumentacije za provjeru valjanosti tvrtki American Express

Svi Trgovci i Davatelji usluga koji moraju sudjelovati u Programu sukladnosti tvrtke American Express moraju poslati dokumentaciju za provjeru valjanosti koja je obilježena kao „obvezna“ u tablicama u [Korak 2: „Razumijevanje Vašeg zahtjeva u vezi Dokumentacije za provjeru valjanosti Razine Trgovca/Davatelja usluge“](#) u American Express do zadanih rokova.

Morate dostaviti Dokumentaciju za provjeru valjanosti tvrtki American Express putem [Portala](#) koji omogućuje Administrator Programa kojeg je odabrao American Express. Kada dostavljate Dokumentaciju za provjeru valjanosti, potvrđujete i jamčite tvrtci American Express da je sljedeće istinito (prema Vašim najboljim saznanjima):

- Vaša je procjena bila potpuna i temeljita;
- Prikazan je točan status PCI DSS-a u trenutku ispunjavanja, bilo da šalje Ovjeru sukladnosti (Attestation of Compliance, AOC) ili PCI Sažetak alata za utvrđivanje prioriteta (PAT) za nesukladnost;
- Vi imate ovlasti za otkrivanje sadržanih informacija i da tvrtki American Express dostavljate Dokumentaciju za provjeru valjanosti bez kršenja prava bilo koje druge stranke.

Naknade za nesukladnost i raskidanje Ugovora

Tvrtka American Express ima pravo naplate naknada za nesukladnost i raskidanje Ugovora ako ne ispunite te zahtjeve ili ako ne isporučite obveznu dokumentaciju za provjeru valjanosti tvrtki American Express do zadanog roka. Tvrtka American Express pokušat će obavijestiti kontakt za sigurnost podataka o važećem roku za svako godišnje i tromjesečno razdoblje.

Tablica A-4: Naknada za nesukladnost

Opis*	Trgovac razine 1 ili Davatelj usluge razine 1	Trgovac razine 2 ili Davatelj usluge razine 2	Trgovac razine 3 ili razine 4
Naknada za nesukladnost procijenit će se ako se Dokumentacija za provjeru valjanosti ne zaprimi do prvog roka.	25.000 USD	5.000 USD	50 USD
Dodatna naknada za nesukladnost procijenit će se ako se Dokumentacija za provjeru valjanosti ne zaprimi do drugog roka.	35.000 USD	10.000 USD	100 USD
Dodatna naknada za nesukladnost procijenit će se ako se Dokumentacija za provjeru valjanosti ne zaprimi do trećeg roka. NAPOMENA: Naknada za nesukladnost primjenjuje se sve dok ne pošaljete Dokumentaciju za provjeru valjanosti.	45.000 USD	15.000 USD	250 USD

* Naknade za nesukladnost procjenjivat će se u Ekvivalentima lokalne valute.

* Ne odnosi se na Argentinu.

Ako Vaše obveze povezane s Dokumentacijom za provjeru sukladnosti PCI DSS-a nisu ispunjene, American Express ima pravo nametnuti naknade za nesukladnost kumulativno, zadržati plaćanja i/ili raskinuti Ugovor.

Odjeljak 3

Obveze za upravljanje Podatkovnim incidentima

Morate odmah obavijestiti tvrtku American Express, u svakom slučaju ne kasnije od sedamdeset dva (72) sata, nakon otkrivanja Podatkovnog incidenta.

Kako biste obavijestili tvrtku American Express, kontaktirajte Program za odziv na incidente tvrtke American Express (American Express Enterprise Incident Response Programme, *EIRP*) na besplatan broj na 1.888.732.3750 ili na 1.602.537.3021 ili pošaljite e-poštu na EIRP@aexp.com. Morate imenovati osobu za kontaktiranje u vezi s takvim Podatkovnim incidentom. Osim toga:

- Morate provesti temeljitu istragu svakog Podatkovnog incidenta hitno poslati u American Express sve Kompromitirane Brojeva Kartica. Tvrtka American Express zadržava pravo na provođenje vlastite interne analize za identificiranje podataka zahvaćenih Podatkovnim incidentom.

Za Podatkovne incidente koji uključuju manje od 10.000 jedinstvenih Brojeva Kartica, sažeto izvješće o provedenoj istrazi treba proslijediti tvrtki American Express u roku od deset (10) radnih dana od sastavljanja.

- Sažeto izvješće o provedenoj istrazi treba sadržavati sljedeće podatke: sažetak incidenta, opis zahvaćenih dokumenata, vremenski tijek događaja, ključni datumi, podaci o utjecaju i izloženosti podataka, radnje za ograničenje i korekciju, potvrda da nema indikacija da su ugroženi dodatni podaci tvrtke American Express.

Ako podatkovni incident obuhvaća 10.000 ili više jedinstvenih Brojeva Kartica, morate angažirati PCI PFI da provede ovu istragu u roku od pet (5) dana od otkrivenog Podatkovnog incidenta.

- Nerevidirano forenzičko izvješće o provedenoj istrazi treba proslijediti tvrtki American Express u roku od deset (10) radnih dana od sastavljanja.
- Forenzička izvješća o provedenoj istrazi moraju biti sastavljena na važećem predlošku za konačna forenzička izvješća o incidentima dostupnom od PCI. Takva izvješća moraju sadržavati forenzičke osvrte, izvješća o sukladnosti i sve druge informacije o Podatkovnom incidentu, identificirati uzrok Podatkovnog incidenta, potvrditi jeste li bili u skladu s PCI DSS-om u trenutku Podatkovnog incidenta ili ne i potvrditi Vašu sposobnost sprječavanja budućih Podatkovnih incidenata (i) pružanjem plana za otklanjanje svih nedostataka u vezi s PCI DSS-om i (ii) sudjelovanjem u programu sukladnosti tvrtke American Express (kako je opisano dolje). Na zahtjev tvrtke American Express morate osigurati provjeru valjanosti koju će provesti Kvalificirani procjenitelj sigurnosti (QSA) kako biste dokazali da su nedostaci otklonjeni.

Bez obzira na prethodne članke ovog [Odjeljak 3. „Obveze za upravljanje Podatkovnim incidentima“](#):

- American Express ima pravo, po vlastitoj procjeni, zahtijevati od Vas da angažirate PFI-ja koji će provesti istragu Podatkovnog incidenta za Podatkovne incidente koji uključuju manje od 10.000 jedinstvenih Brojeva Kartica ili gdje se dogodilo više incidenata u razdoblju od 12 mjeseci. Sve takve istrage moraju biti u skladu sa zahtjevima navedenima u ovom [Odjeljak 3. „Obveze za upravljanje Podatkovnim incidentima“](#) i moraju se dovršiti u vremenskom okviru koji odredi tvrtka American Express.
- Tvrtka American Express može, po vlastitom nahođenju, zasebno angažirati PFI-ja za provođenje istrage za bilo koji „Podatkovni incident“ i teretiti Vas za trošak takve istrage.

Podatkovni incident morate procijeniti prema važećim globalnim zakonima o obavješćivanju o povredi podataka i gdje se smatra potrebnim, obavijestiti važeća regulatorna tijela i zahvaćene Korisnike u skladu s tim zakonima o obavješćivanju o povredi podataka. Ako ste utvrdili da je Vaš Davatelj usluga ili drugi subjekt odgovoran za prijavu Podatkovnog incidenta, morate obavijestiti tog Davatelja usluga ili subjekt o njegovoj dužnosti da procijeni svoje obveze izvješćivanja prema važećim zakonima o obavješćivanju o povredi podataka. Suglasni ste da ćete od tvrtke American Express dobiti pisano odobrenje prije spominjanja ili imenovanja tvrtke American Express u bilo kojoj komunikaciji s Korisnicima o Podatkovnom incidentu. Pristajete surađivati s tvrtkom American Express kako biste pružili podatke i otklonili sve probleme proizašle iz Podatkovnog incidenta, uključujući pružanje (i pribavljanje svih neophodnih odricanja od odgovornosti) koje sadrže za American Express sve relevantne podatke za provjeru Vaše sposobnosti za sprječavanje budućih Podatkovnih incidenata na način sukladan Ugovoru.

Bez obzira na bilo kakvu proturječnu obvezu povjerljivosti u Ugovoru, tvrtka American Express ima pravo na otkrivanje informacija o bilo kojem Podatkovnom incidentu Korisnicima usluge kartičnog plaćanja American Express, Izdavateljima i drugim sudionicima mreže American Express te općoj javnosti, u skladu s Primjenjivim zakonom; sudskim, administrativnim ili pravnim nalogom, proglasom, sudskim pozivom, zahtjevom ili drugim postupkom radi smanjenja opasnosti od prijevare ili drugih ugroza ili na drugi način do obima prikladnog za upravljanje Mrežom American Express.

Što učiniti ako imate Podatkovni incident?

Poduzmite ove poteze ako ste identificirali Podatkovni incident u svojoj tvrtki.



Potez 1:

Popunite Obrazac [za obavijest o incidentu s podacima o](#) Trgovcu i pošaljite ga na EIRP@aexp.com u roku od 72 sata nakon otkrivanja Podatkovnog incidenta.



Potez 2:

Provedite temeljitu istragu. Može biti potrebno da angažirate Forenzičkog istražitelja [u oblasti industrije platnih kartica \(Payment Card Industry, PCI\)](#).



Potez 3:

Odmah nam dostavite sve ugrožene brojeve Kartica American Express®.



Potez 4:

Radite s nama kako biste pomogli u rješavanju svih problema koji proizlaze iz Podatkovnog incidenta.

Vidite [Odjeljak 3. „Obveze za upravljanje Podatkovnim incidentima“](#) za više pojedinosti o Obvezama upravljanja Podatkovnim incidentima.

Imate li još pitanja?

SAD: (888) 732-3750 (broj za besplatni poziv)

Međunarodno: +1 (602) 537-3021

EIRP@aexp.com

Odjeljak 4 Obveze obeštećenja zbog Podatkovnog incidenta

Vaše obveze obeštećenja prema tvrtki American Express utvrđene su Ugovorom s tvrtkom American Express za „Podatkovne incidente“, bez poništavanja bilo kojih drugih prava ili mjera tvrtke American Express u okviru ovog [Odjeljak 4. „Obveze obeštećenja zbog Podatkovnog incidenta“](#). Osim obveza obeštećenja (ako postoje), možda ćete morati platiti naknadu za nesukladnost Podatkovnog incidenta kako je opisano u nastavku u [Odjeljak 4. „Obveze obeštećenja zbog Podatkovnog incidenta“](#).

Tvrtku American Express ćete obeštetiti po cijeni od 5 USD po broju računa, za Podatkovne incidente koji obuhvaćaju:

- 10.000 ili više Brojeva Kartica American Express koji sadrže nešto od sljedećeg:
 - Osjetljivi podaci za provjeru autentičnosti, ili
 - Datum isteka

Međutim, American Express neće od vas zahtijevati obeštećenje za Podatkovni incident koji obuhvaća:

- manje od 10.000 Brojeva Kartice American Express ili
- više od 10.000 Brojeva Kartice American Express, ako zadovoljite sljedeće uvjete:
 - obavijestili ste American Express o Podatkovnom incidentu u skladu s [Odjeljak 3. „Obveze za upravljanje Podatkovnim incidentima“](#),
 - djelovali ste sukladno s PCI DSS-om u vrijeme Podatkovnog incidenta (što se utvrđuje istragom PFI-ja o Podatkovnom incidentu) i
 - Podatkovni incident nije bio uzrokovan pogrešnim postupanjem Vas ili Vaših Obuhvaćenih stranaka.

Bez obzira na prethodne članke ovog [Odjeljak 4. „Obveze obeštećenja zbog Podatkovnog incidenta“](#), za svaki Podatkovni incident, neovisno o količini Brojeva Kartica American Express, tvrtki American Express ćete platiti Naknadu za Podatkovni incident zbog nesukladnosti koja neće premašivati USD 100.000\$ po Podatkovnom

incidentu (kako utvrđuje tvrtka American Express po vlastitoj procjeni) ako ne budete djelovati sukladno s bilo kojom od svojih obveza navedenih u [Odjeljak 3. „Obveze za upravljanje Podatkovnim incidentima“](#). Kako bi se izbjegle nedoumice, ukupna naknada za nesukladnost Podatkovnog incidenta procijenjena za bilo koji Podatkovni incident ne smije biti viša od USD 100.000\$.

Tvrtka American Express iz svojih će izračuna isključiti sve Brojeve računa Kartica American Express koji su bili uvršteni u prethodni zahtjev za obeštećenje za Podatkovni incident podnesen u roku od dvanaest (12) mjeseci prije Datuma obavijesti. Svi izračuni koje ovom metodologijom izvrši tvrtka American Express su konačni.

Tvrtka American Express može Vam naplatiti cijeli iznos obveza obeštećenja za Podatkovne incidente ili umanjiti iznos isplata tvrtke American Express Vama (ili na temelju njega zadužiti Vaš bankovni račun) sukladno s Ugovorom.

Ovdje navedene Vaše obveze za obeštećenjem za Podatkovne incidente ne smatraju se slučajnim, neizravnim, spekulativnim, posljedičnim, posebnim, kaznenim ili primjernim štetama u okviru Ugovora, pod uvjetom da takve obveze ne obuhvaćaju štete koje su u naravi gubitka dobiti ili prihoda, dobre volje ili poslovnih prilika odnosno povezane s njima.

American Express po vlastitom nahođenju može smanjiti obvezu za obeštećenjem samo za Trgovce za Podatkovne incidente koji zadovoljavaju sljedeće kriterije:

- Prije Podatkovnog incidenta uporabljene su primjenjive Tehnologije za izbjegavanje rizika i koristile su se tijekom cijelog Vremenskog okvira Podatkovnog incidenta,
- Provedena je temeljita istraga u skladu s programom PFI (osim ako je prethodno pismenim putem ugovoreno drugačije),
- U forenzičkom izvješću jasno se navodi da su se za obradu, spremanje i/ili prijenos podataka u vrijeme Podatkovnog incidenta koristile Tehnologije za izbjegavanje rizika i
- Ne spremate (i niste tijekom trajanja vremenskog okvira Podatkovnog incidenta spremali) osjetljive podatke za provjeru autentičnosti i Podatke Vlasnika kartica koji nisu bili šifrirani.

Kada je dostupno smanjenje obeštećenja, smanjenje Vaše obveze za obeštećenjem (isključujući naplative naknade zbog nesukladnosti) utvrđuje se prema sljedećem:

Tablica A-5: Kriterij za smanjenje obveze za obeštećenjem

Smanjenje obveze za obeštećenjem	Potrebni kriterij
Standardno smanjenje: 50 %	>75% ukupnih Transakcija obrađenih na Uređajima koji podržavaju čipove ¹ ILI Tehnologija za izbjegavanje rizika koristi se na >75% lokacija Trgovca ²
Poboljšano smanjenje: 75% do 100%	>75% svih Transakcija obrađenih na Uređajima koji podržavaju čipove ¹ I druga Tehnologija za izbjegavanje rizika koja se koristi na >75% lokacija Trgovca ²

¹ Utvrđuje se internom analizom tvrtke American Express

² Utvrđuje se PFI istragom

- Poboljšano smanjenje (75% do 100%) se utvrđuje na temelju manjeg postotka Transakcija s pomoću Uređaja koji podržavaju čipove i lokacija Trgovaca na kojima se koristi druga Tehnologija za izbjegavanje rizika. Primjeri u [Tablica A-6: Smanjenje povećane obveze za obeštećenjem](#) prikazuje izračun smanjenja obeštećenja.
- Kako biste ispunjavali uvjete za uporabu Tehnologije za izbjegavanje rizika, morate dokazati učinkovitu primjenu tehnologije u skladu s njezinim dizajnom i namjenom.
- Postotak Vaših lokacija na kojima se koristi Tehnologija za izbjegavanje rizika utvrđuje se PFI istragom.

- Smanjenje obveze za obeštećenjem ne vrijedi ni za kakve naplative naknade zbog nesukladnosti u vezi s Podatkovnim incidentom.

Tablica A-6: Smanjenje povećane obveze za obeštećenjem

Primjer	Uporaba Tehnologije za izbjegavanje rizika	Prikladni	Smanjenje
1	80% Transakcija na Uređajima koji podržavaju čipove 0% lokacija rabi drugu Tehnologiju za izbjegavanje rizika	Ne	50%: Standardno smanjenje (uporaba manje od 75% Tehnologije za izbjegavanje rizika ne ispunjava uvjete za poboljšano smanjenje) ¹
2	80% Transakcija na Uređajima koji podržavaju čipove 77% lokacija rabi drugu Tehnologiju za izbjegavanje rizika	Da	77%: Poboljšano smanjenje (na temelju 77% uporabe Tehnologije za izbjegavanje rizika)
3	93% Transakcija na Uređajima koji podržavaju čipove 100% lokacija rabi drugu Tehnologiju za izbjegavanje rizika	Da	93%: Poboljšano smanjenje (na temelju 93% Transakcija na Uređajima koji podržavaju čipove)
4	40% Transakcija na Uređajima koji podržavaju čipove 90% lokacija rabi drugu Tehnologiju za izbjegavanje rizika	Ne	50%: Standardno smanjenje (manje od 75% Transakcija na Uređajima koji podržavaju čipove ne ispunjava uvjete za poboljšano smanjenje)

¹ Podatkovni incident koji obuhvaća 10.000 računa Kartica American Express, po cijeni od 5 USD po broju računa (10.000 x 5 USD = 50.000 USD) može ispunjavati uvjete za smanjenje od 50%, smanjujući obveze za obeštećenjem s 50.000 USD na 25.000 USD, isključujući sve naknade za nesukladnost.

Odjeljak 5

Program ciljane analize (TAP)

Kompromitiranje podataka vlasnika kartice može biti uzrokovano propustima u sigurnosti u Vašem Podatkovnom okruženju vlasnika kartice (CDE).

Primjeri kompromitiranja Podataka vlasnika kartica uključuju, ali nisu ograničeni na:

- **Učestale točke kupnje (CPP):** Korisnici usluga kartičnog plaćanja tvrtke American Express prijavljuju prijevarene Transakcije na svojim Kartičnim računima i one se identificiraju i utvrđuje se da vode podrijetlo iz vršenja kupnje u Vašim poslovnica.
- **Pronađeni Kartični podaci:** Pronađeni kartični i podaci vlasnika Kartica American Express na svjetskoj mreži povezani s transakcijama u Vašim poslovnica.
- **Sumnja na zlonamjerni softver:** American Express sumnja da rabite softver zaražen sa ili osjetljiv na zlonamjerni kod.

Program ciljane analize (TAP) je osmišljen da identificira potencijalno Kompromitiranje podataka vlasnika kartice.

Morate osigurati da i Vaše Obuhvaćene strane poštuju sljedeće zahtjeve nakon obavijesti od tvrtke American Express o potencijalnom Kompromitiranju Podataka vlasnika kartice.

- Morate hitno pregledati da u Vašem CDE nema propusta u sigurnosti podataka i korigirati sve eventualne nalaze.
 - Morate dovesti do toga da dobavljač(i) kao treće strane izvrše temeljitu istragu Vašeg CDE, ukoliko je on nabavljen od trećih strana.
- Morate pružiti sažetak poduzetih ili planiranih radnji iz svojih napora na pregledu, evaluaciji i/ili korekciji po obavijesti od tvrtke American Express.
- Morate pružiti ažurirane dokumente za provjeru valjanosti PCI DSS sukladno s [Odjeljak 2. „PCI DSS program sukladnosti \(Važna periodična provjera valjanosti Vaših sustava\)“](#).
- Ako je primjenjivo, morate angažirati kvalificiranog PCI PFI da ispita Vaš CDE ako Vi ili Vaša Obuhvaćena strana:
 - ne može riješiti kompromitiranje podataka vlasnika kartice u razumnom roku, kako je utvrdila tvrtka American Express ili
 - potvrđujete da se dogodio Podatkovni incident i da je sukladan zahtjevima postavljenima u [Odjeljak 3. „Obveze za upravljanje Podatkovnim incidentima“](#).

Tablica A-7: TAP naknada za nesukladnost

Opis	Trgovac razine 1 ili Davatelj usluge razine 1	Trgovac razine 2 ili Davatelj usluge razine 2	Trgovac razine 3 ili razine 4
Naknada za nesukladnost procijenit će se kada TAP obveze nisu ispunjene do prvog roka.	25.000 USD	5.000 USD	1.000 USD
Naknada za nesukladnost procijenit će se kada TAP obveze nisu ispunjene do drugog roka.	35.000 USD	10.000 USD	2.500 USD
Naknada za nesukladnost procijenit će se kada TAP obveze nisu ispunjene do trećeg roka. NAPOMENA: Naknade za nesukladnost mogu se i dalje primjenjivati dok se ne ispune obveze ili dok se TAP ne riješi.	45.000 USD	15.000 USD	5.000 USD

Ako Vaše TAP obveze nisu ispunjene, American Express ima pravo nametnuti naknade za nepoštivanje kumulativno, zadržati plaćanja i/ili raskinuti Ugovor.

Odjeljak 6

Povjerljivost

Tvrtka American Express poduzet će razumne mjere da vaša izvješća o sukladnosti, uključujući da Dokumentaciju za provjeru valjanosti zadrže (što vrijedi i za njihove predstavnike i podugovorene stranke, uključujući pružatelja usluga Portala) povjerljivima i da Dokumentaciju za provjeru valjanosti neće otkrivati nijednoj trećoj strani (osim Pridruženih tvrtki, agenata, predstavnika, Davatelja usluge i podugovorenih stranki) u razdoblju od tri godine od datuma zaprimanja, osim što ova obveza o povjerljivosti ne vrijedi za Dokumentaciju za provjeru valjanosti:

- koja je tvrtki American Express već bila poznata prije otkrivanja,
- koja jest ili postane dostupna javnosti od strane tvrtke American Express bez kršenja ovog članka,
- koju je tvrtka American Express valjano zaprimila od treće strane bez obveze za povjerljivost,
- koju je neovisno razvila tvrtka American Express ili
- koju treba otkriti po nalogu suda, upravnog organa ili vladinog tijela, ili tako nalaže bilo koji zakon, propis ili uredba ili sudski poziv, zahtjev za otkrivanjem, opoziv ili drugi upravni ili pravni postupak ili bilo koji službeni ili neslužbeni zahtjev ili istraga bilo koje vladine agencije ili tijela (uključujući sve regulatore, inspektore, revizore ili agencije za provedbu zakona).

Odjeljak 7 Odricanje od odgovornosti

TVRTKA AMERICAN EXPRESS OVIM SE PUTEM ODRIČE BILO KOJIH I SVIH REPREZENTACIJA, JAMSTAVA I ODGOVORNOSTI U POGLEDU OVOG RADNOG PRAVILNIKA ZA SIGURNOST PODATAKA, PCI DSS-a, „EMV SPECIFIKACIJE“ I NAMJENE TE IZVEDBE QSA-ova, ASV-ova ILI PFI-ova (ILI BILO KOJEG OD NJIH), BILO IZREČENO, PODRAZUMIJEVANO, ZAKONSKI ILI DRUGAČIJE, UKLJUČUJUĆI SVA JAMSTVA O MOGUĆNOSTI PRODAJE ILI ODGOVARANJA ODREĐENOJ SVRSI. IZDAVATELJI KARTICA AMERICAN EXPRESS NISU KORISNICI TREĆE STRANE U OKVIRU OVOG PRAVILNIKA.

Odjeljak 8 Pojmovnik

Samo za svrhu *Radnog pravilnika za sigurnost podataka*, važe i kontroliraju se sljedeće definicije:

Aplikacija za plaćanje ima značenje kako je navedeno u aktualnom Pojmovniku termina za Standarde platnih kartica Secure Software i Secure Software Life Cycle, koji su dostupni na www.pcisecuritystandards.org.

Broj kartice znači jedinstveni identifikacijski broj kojeg Izdavalatelj dodjeljuje Kartici kod izdavanja.

Čip se odnosi na integrirani mikročip na Kartici koji sadrži informacije o Korisniku usluge Kartičnog plaćanja i računu.

Datum obavijesti odnosi se na datum na koji tvrtka American Express izdavalateljima pošalje završnu obavijest o Podatkovnom incidentu. Takav datum ovisi o tome kada tvrtka American Express zaprimi završno forenzičko izvješće ili rezultate interne analize i po vlastitoj ga prosudbi određuje tvrtka American Express.

Davatelj franšize se odnosi na operatera tvrtke koja licencira osobe ili Subjekte (Primatelji franšize) za distribuciju robe i/ili usluga pod ili s uporabom operaterove oznake, pomažu Primateljima franšize u poslovanju ili utječu na način poslovanja franšize i od Primatelja franšize zahtijeva plaćanje naknade.

Davatelji usluge odnosi se na procesore, procesore trećih strana, davatelje usluge pristupnika, integratore POS sustava i sve druge davatelje usluga Trgovcima ili POS sustavima ili druga rješenja ili usluge za obradu plaćanja.

Davatelj usluge razine 1 odnosi se na Davatelja usluge s 2,5 milijuna ili više Transakcija putem Kartice American Express na godinu ili na Davatelja usluge kojeg tvrtka American Express inače smatra Davateljem usluge Razine 1.

Davatelj usluge razine 2 odnosi se na Davatelja usluge s manje od 2,5 milijuna Transakcija putem Kartice American Express na godinu ili na sve Davatelje usluge koje tvrtka American Express ne smatra Davateljima usluge Razine 1.

Dokumentacija za provjeru valjanosti odnosi se na AOC dobiven u vezi s Godišnjom procjenom sigurnosti na lokaciji ili SAQ-om, AOSC-om i izvršnim sažecima nalaza dobivenim u vezi s Tromjesečnim skeniranjima Mreže ili Godišnjom ovjerom Programa za unaprjeđenje sigurnosne tehnologije.

EMV specifikacije odnose se na specifikacije koje izdaje EMVCo, LLC i koje su dostupne na www.emvco.com.

EMV transakcija odnosi se na Transakciju putem kartice s integriranim krugom (ponekad se naziva i „IC kartica“, „kartica sa čipom“, „pametna kartica“, „EMV kartica“ ili „ICC“) izvršenu na terminalu na točki prodaje (POS) koja podržava IC karticu s valjanim odobrenjem EMV tipa. Odobrenje EMV tipa dostupna su na www.emvco.com.

Izdavalatelj kartice označava bilo koji Subjekt (uključujući tvrtku American Express i njezina povezana lica) koji ima licencu od strane tvrtke American Express ili povezanog lica tvrtke American Express za izdavanje Kartica i za angažiranje u djelatnosti izdavanja Kartica.

Kartica American Express ili **Kartica** odnosi se na bilo koju karticu, uređaj za pristup računu, platni uređaj ili uslugu s nazivom, logotipom, zaštitnim znakom, znakom usluge, trgovačkim nazivom ili drugim vlasničkim dizajnom ili oznakom tvrtke American Express ili pridružene tvrtke koje izdaje izdavalatelj ili se nalaze na računu kartice.

Kartica sa čipom odnosi se na Karticu koja sadrži čip i za koju može biti potreban PIN kao sredstvo ovjere identiteta korisnika usluge kartičnog plaćanja ili informacija o računu koje čip sadrži ili ovoje (ponekad se u našim materijalima naziva „pametna kartica“, „EMV kartica“, „ICC“ ili „kartica s integriranim krugom“).

Ključ za šifriranje (Ključ za šifriranje American Express) odnosi se na sve ključeve koji se koriste u obradi, generiranju, učitavanju i/ili zaštiti podataka na računu. To uključuje između ostalog sljedeće:

- Ključevi za šifriranje: Glavni ključevi zone (Zone Master Keys, ZMK-ovi) i PIN ključevi zone (Zone Pin Keys, ZPK-ovi)
- Glavni ključevi koji se koriste za osiguravanje kriptografskog uređaja: Lokalni glavni ključevi (Local Master Keys, LMK-ovi)
- Ključevi sigurnosnog koda kartice (Card Security Code Keys, CSMK-ovi)
- PIN ključevi: Osnovni derivirani ključevi (Base Derivation Keys, BDK-ovi), ključevi za šifriranje PIN-a (PIN Encryption Keys, PEK-ovi) i ZPK-ovi

Kompromitirani broj kartice odnosi se na broj kartičnog računa American Express povezan s Podatkovnim incidentom.

Korisnik usluge kartičnog plaćanja označava pojedinca ili subjekt (1) koji je sklopio ugovor otvaranjem Kartičnog računa s izdavateljem ili (2) čije se ime nalazi na Kartici.

Kredit se odnosi na iznos koji vraćate Korisnicima usluge kartičnog plaćanja za kupnje ili plaćanja izvršena Karticom.

Kreditni zapis znači zapis Kredita koji je u skladu s našim zahtjevima.

Kvalificirani procjenitelj sigurnosti (QSA) označava subjekt koji je kvalificirao Payment Card Industry Security Standards Council, LLC za ovjeru ispunjavanja PCI DSS-a.

Naplata se odnosi na plaćanje izvršeno Karticom.

Obuhvaćene stranke odnosi se na sve vaše zaposlenike, agente, predstavnike, podugovaratelje, procesore, davatelje usluge, dobavljače vaše opreme na točki prodaje (POS), sustave ili rješenja za obradu plaćanja, Subjekte povezane s vašim trgovačkim računom American Express i sve druge stranke kojima možete posredovati pristup Podacima vlasnika kartice ili Osjetljivim podacima za provjeru autentičnosti (ili oboje)u skladu s Ugovorom.

Odobreni skeniratelj (ASV) označava Subjekt koji je kvalificirao Payment Card Industry Security Standards Council, LLC za ovjeru ispunjavanja određenih zahtjeva PCI DSS-a provođenjem skeniranja ranjivosti okruženja povezanih s internetom.

Odobreno rješenje za šifriranje od točke do točke (P2PE), uključeno je na PCI SSC popisu ovjerenih rješenja ili rješenje koje ovjerava Tvrtka koja je temeljem PCI SSC-a ovlaštena za procjenu sigurnosti P2PE-a.

Osjetljivi podaci za provjeru autentičnosti označava podatke povezane sa sigurnošću koji se koriste za provjeru autentičnosti vlasnika kartice i/ili autorizaciju transakcija platnom karticom. Ti podaci sadrže, ali nisu ograničeni na verifikacijske kodove kartice, pune podatke za praćenje (s magnetske trake ili ekvivalenta na čipu), PIN-ove i blokove PIN-a.

Ovjera sukladnosti (AOC) označava izjavu o statusu vaše sukladnosti s PCI DSS-om u obrascu koji pribavlja Payment Card Industry Security Standards Council, LLC.

Ovjera sukladnosti (AOSC) označava izjavu o statusu vaše sukladnosti s PCI DSS-om na temelju mrežnog skeniranja, u obrascu koji pribavlja Payment Card Industry Security Standards Council, LLC.

Payment Card Industry Data Security Standard (PCI DSS) odnosi se na Standard za sigurnost podataka u industriji platnih kartica koji je dostupan na www.pcisecuritystandards.org.

PCI DSS odnosi se na Standard za sigurnost podataka u industriji platnih kartica koji je dostupan na www.pcisecuritystandards.org.

PCI forenzički istražitelj (PFI) odnosi se na subjekt kojeg je odobrio Payment Card Industry Security Standards Council, LLC za vršenje forenzičkih istraga u slučaju kršenja ili kompromitiranja podataka platnih kartica.

PCI odobreno znači da se Uređaj za unos PIN-a ili Aplikacija za plaćanje (ili oboje) u vrijeme uporabe nalaze na popisu odobrenih tvrtki i davatelja usluge koji održava PCI Security Standards Council, LLC, koji je dostupan na www.pcisecuritystandards.org.

Podaci o korisniku usluge kartičnog plaćanja odnosi se na podatke o korisnicima usluge kartičnog plaćanja i transakcija putem kartice, uključujući ime, adresu, broj računa kartice i identifikacijski broj kartice (CID).

Podaci računa sastoje se od Podataka vlasnika kartice i/ili Osjetljivi podaci za provjeru autentičnosti. Pogledajte Podaci vlasnika kartice i Osjetljivi podaci za provjeru autentičnosti.

Podaci transakcije označava sve podatke koje zahtijeva American Express, koji dokazuju jednu ili više Transakcija, uključujući podatke dobivene na prodajnom mjestu, podatke dobivene ili generirane tijekom Autorizacije i Slanja i bilo koji povrat.

Podaci vlasnika kartice označava najmanje puni Stalni broj računa (PAN) sam ili puni PAN plus bilo što od sljedećeg: ime i prezime vlasnika kartice, datum isteka i/ili servisni broj. Pogledajte Osjetljivi podaci za provjeru autentičnosti koji bi se mogli prenositi ili obrađivati (ali ne i pohranjivati) o okviru transakcije plaćanja.

Podatkovni incident odnosi se na incident koji uključuje kompromitiranje ili sumnju na kompromitiranje ključeva za šifriranje American Express ili barem jednog kartičnog računa American Express na kojem je došlo do:

- neovlaštenog pristupa ili uporabe Ključeva za šifriranje, Podataka vlasnika kartice ili Osjetljivih podataka za provjeru autentičnosti (ili kombinacija navedenog) koji se spremaju obrađuju ili šalju putem vaše opreme, sustava i/ili mreža (i njihovih komponenti) ili njihovom uporabom pod vašim nadzorom ili koje pružate ili činite dostupnim,
- uporabe Ključeva za šifriranje, Podataka vlasnika kartice ili Osjetljivih podataka za provjeru autentičnosti (ili kombinacija navedenog) koja nije u skladu s Ugovorom, i/ili
- mogućeg ili potvrđenog gubitka, krađe, pronevjere na bilo koji način putem bilo kojeg medija, materijala, zapisa ili informacija sadržanih u takvim Ključevima za šifriranje, Podacima vlasnika kartice ili Osjetljivim podacima za provjeru autentičnosti (ili kombinacija navedenog).

Podatkovno okruženje vlasnika kartice (CDE) odnosi se na ljude, procese i tehnologiju koji pohranjuju, obrađuju ili prenose podatke vlasnika kartice ili osjetljive podatke za provjeru autentičnosti.

Portal znači sustav izvješćivanja koji omogućuje administrator Programa PCI u tvrtki American Express kojeg je odabrala tvrtka American Express. Trgovci i Davatelji usluga obvezni su koristiti se Portalom za slanje PCI dokumentacije za provjeru valjanosti tvrtki American Express.

Predložak za konačna forenzička izvješća o incidentima znači predložak koji omogućava PCI Security Standards Council, dostupan na stranici www.pcisecuritystandards.org.

Primatelj franšize znači treću stranu koja je u neovisnom vlasništvu i neovisno se vodi (uključujući Davatelja franšize, vlasnika licence ili poglavlje) koji nisu Povezana strana koja ima licencu od Davatelja franšize za vođenje franšize i koja je stupila u pismeni ugovor s Davateljem franšize sukladno s kojim kontinuirano prikazuje eksterne informacije i istaknuto se identificira sa markama Davatelja franšize, ili se prikazuje u javnosti kao član skupine tvrtki Davatelja franšize.

Procesor se odnosi na davatelja usluge koji Trgovcu obavlja autorizaciju i obradu slanja u mrežu American Express.

Program znači Program sukladnosti tvrtke American Express s PCI-jem.

Program ciljane analize odnosi se na program koji omogućuje ranu identifikaciju potencijalnog Kompromitiranja podataka vlasnika kartice u vašem Podatkovnom okruženju vlasnika kartice (CDE). Vidite [Odjeljak 5. „Program ciljane analize \(TAP\)“](#).

Program za unaprjeđenje sigurnosne tehnologije (STEP) odnosi se na program tvrtke American Express kojim se Trgovci potiču na razvoj tehnologija koje unaprjeđuju sigurnost podataka.

Potrošač se definira kao vlasnik kartice koji kupuje robu, usluge ili oboje.

Razina trgovca znači klasifikacija dodijeljena trgovcu ovisno o njegovim obvezama za provjeru sukladnosti PCI DSS-a, kao u [Odjeljku 2. „PCI DSS program sukladnosti \(Važna periodična provjera valjanosti Vaših sustava\)“](#).

Šifriranje od točke do točke (P2PE) odnosi se na rješenje koje kriptografski štiti podatke računa od točke u kojoj trgovac prihvaća platnu karticu do sigurne točke dešifriranja.

Sigurnosni zahtjevi za PCI PIN odnosi se na Sigurnosne zahtjeve za PIN u industriji Platnih kartica koji je dostupan na www.pcisecuritystandards.org.

Stalni broj računa (PAN) ima značenje navedeno u trenutačnom pojmovniku PCI DSS-a.

Sustav točaka prodaje (POS) odnosi se na sustav ili opremu za obradu informacija, uključujući terminal, osobno računalo, elektroničku blagajnu, beskontaktni čitač ili platni mehanizam ili postupak koji koristi Trgovac za pribavljanje autorizacije ili prikupljanje podataka Transakcije ili oboje.

Tehnologija za izbjegavanje rizika odnosi se na tehnološka rješenja koja unapređuju sigurnost Podataka Vlasnika Kartice American Express i osjetljivih Podataka za provjeru autentičnosti, kako utvrđuje tvrtka American Express. Kako biste ispunjavali uvjete za uporabu Tehnologije za izbjegavanje rizika, morate dokazati učinkovitu primjenu tehnologije u skladu s njezinim dizajnom i namjenom. Primjeri uključuju, među ostalim: EMV, Šifriranje od točke do točke i tokenizacija.

Token znači kriptografski token koji zamjenjuje PAN na temelju navedenog indeksa za nepredvidivu vrijednost.

Transakcija označava Naplatu, Kredit, gotovinski predujam (ili drugi pristup gotovini) ili bankomatska Transakcija obavljena s pomoću Kartice.

Transakcije koje pokreće kupac (BIP) označava sustav za digitalno plaćanje koji kupcima omogućuje brzo i učinkovito zakazivanje plaćanja dobavljačima (povezano s korporativnim karticama).

Trgovac se odnosi na Trgovca i sve njegove pridružene tvrtke koje prihvaćaju Karticu American Express u skladu s Ugovorom s tvrtkom American Express ili njezinim pridruženim tvrtkama.

Trgovac razine 1 odnosi se na Trgovca s 2,5 milijuna ili više Transakcija putem Kartice American Express godišnje ili na Trgovca kojeg tvrtka American Express inače smatra Trgovcem razine 1.

Trgovac razine 2 odnosi se na Trgovca s 50.000 do manje od 2,5 milijuna Transakcija putem Kartice American Express godišnje.

Trgovac razine 3 odnosi se na Trgovca s 10.000 do manje od 50.000 Transakcija putem Kartice American Express godišnje.

Trgovac razine 4 odnosi se na Trgovca s manje od 10.000 Transakcija putem Kartice American Express godišnje.

Ugovor označava Opće odredbe, Propisi za Trgovce i sve prateće planove i priloge, zajedno (ponekad se u našim materijalima naziva Ugovor o prihvaćanju kartica).

Upitnik za samoprocjenu (SAQ) odnosi se na alat za samoprocjenu koji je izradio Payment Card Industry Security Standards Council, LLC, namijenjen procjeni i ovjeri sukladnosti s PCI DSS-om.

Uređaj koji podržava čipove odnosi se na uređaj na točki prodaje s valjanim i trenutačnim EMVCo (www.emvco.com) odobrenjem/certifikatom i koji može obrađivati transakcije s karticama sa čipom u skladu s AEIPS-om.

Uređaj za unos PIN-a ima značenje kako je navedeno u Pojmovniku za sigurnost transakcija s PIN-om u industriji platnih kartica (PIN Transaction Security, PTS), točku interakcije (Point of Interaction, POI), zahtjeve za modularnu sigurnost, koji je dostupan na www.pcisecuritystandards.org.

Vlasnik kartice označava kupca kojemu je izdana platna kartica ili bilo koju osobu ovlaštenu za korištenje platne kartice

Vremenski okvir podatkovnog incidenta podrazumijeva vremenski okvir protupravnog ulaganja (ili sličnog određenog vremenskog razdoblja) koji je naveden u konačnom forenzičkom izvješću (npr. PFI izvješće), ili ako nije poznato, do 365 dana prije Datuma zadnje obavijesti o potencijalno Kompromitiranim brojevima kartica uključenim u izvještaj o Kompromitiranim podacima koji nam je dostavljen.

Zahtjevi Payment Card Industry Security Standards Council (PCI SSC) odnosi se na skup standarda i zahtjeva koji se tiču osiguravanja i zaštite podataka platne kartice, uključujući PCI DSS i PA DSS, a dostupni su na www.pcisecuritystandards.org.

Zapis o naplati označava ponovljiv (papirnat i elektronički) zapis o Naplati koji je u skladu s našim zahtjevima i sadrži Broj Kartice, datum Transakcije, Iznos u dolarima, Odobrenje, potpis Vlasnika kartice (ako je primjenjivo) i druge podatke.

Odjeljak 9 Korisna web-mjesta

Sigurnost podataka tvrtke American Express: www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

EMVCo: www.emvco.com