

Radni pravilnik za sigurnost podataka (DSOP)

Kao lider u zaštiti potrošača, tvrtka American Express oduvijek se zalaže za zaštitu „podataka vlasnika kartice“ i „osjetljivih podataka za provjeru autentičnosti“ i 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, 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“, 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.

Odjeljak 1 Standardi za zaštitu „ključeva za šifriranje“, „podataka vlasnika kartice“ i „osjetljivih podataka za provjeru autentičnosti“

Vi i vaše „pokrivenne stranke“ morate:

- spremati „podatke vlasnika kartice“ samo za vršenje „transakcija“ putem kartice American Express i u skladu s ugovorom i kako je zahtijevano njime.
- biti u skladu s trenutnim PCI DSS-om i drugim zahtjevima PCI SSC koji se mogu primijeniti na obradu, spremanje ili prijenos podataka vlasnika kartica ili osjetljivih podataka za provjeru autentičnosti ne kasnije od datuma stupanja na snagu za uvođenje te verzije važećeg zahtjeva.
- koristiti samo na mjestu prisustva koja su „PCI odobrena“ prilikom uvođenja novih ili zamjene „uređaja za unos PIN-a“ ili „aplikacija za plaćanje“ (ili oboje).

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 „pokrivenih stranaka“ s ovim odredbama za sigurnost podataka (umjesto iskazivanja sukladnosti vaših „pokrivenih stranaka“ s ovim pravilnikom u okviru [Odjeljak 4. „Važna redovita provjera valjanosti vaših sustava“](#), osim ako se u tom odjeljku ne navodi drugačije).

Odjeljak 2 Obveze za upravljanje podatkovnim incidentima

Morate odmah obavijestiti tvrtku American Express, u svakom slučaju ne kasnije od dvadeset i četiri (24) sata, nakon otkrivanja „podatkovnog incidenta“.

Kako biste kontaktirali tvrtku American Express, kontaktirajte program za odziv na incidente tvrtke American Express (American Express Enterprise Incident Response Programme, *EIRP*) na +1 (602) 537-3021 (+ označava prefiks za izravno međunarodno biranje „IDD“, naplaćuje se naknada za međunarodne pozive) ili putem e-pošte na EIRP@aexp.com. Morate imenovati osobu za kontaktiranje u vezi s „podatkovnim incidentom“. Osim toga:

- Morate provesti temeljitu forenzičku istragu podatkovnog incidenta.
- Ako podatkovni incident obuhvaća 10.000 ili više jedinstvenih brojeva računa kartica, morate angažirati forenzičara za PCI (PCI Forensic Investigator, PFI) koji će provesti istragu u roku od pet (5) dana od saznanja o podatkovnom incidentu.
- Nerevidirano forenzičko izvješće o provedenoj istrazi treba proslijediti tvrtki American Express u roku od deset (10) radnih dana od sastavljanja.
- Tvrtki American Express morate što prije poslati sve „kompromitirane brojeve kartica“. Tvrtka American Express zadržava pravo na provođenje vlastite interne analize za identificiranje brojeva kartica zahvaćenih „podatkovnim incidentom“.

Forenzička izvješća o provedenoj istrazi moraju biti sastavljena na važećem predlošku za konačna forenzička izvješća o incidentima u skladu sa standardom 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) navođenjem 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 validaciju koju će provesti „kvalificirani procjenitelj sigurnosti“ (Qualified Security Assessor, QSA) kako biste dokazali da su nedostaci otklonjeni.

Bez obzira na prethodne članke ovog [Odjeljak 2. „Obveze za upravljanje podatkovnim incidentima“](#):

- tvrtka 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. Sve takve istrage moraju biti u skladu sa zahtjevima navedenima u ovom [Odjeljak 2. „Obveze za upravljanje podatkovnim incidentima“](#) i dovršiti se 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.

Pristajete surađivati s tvrtkom American Express kako biste otklonili sve probleme proizašle iz „podatkovnog incidenta“, uključujući i savjetovanje s tvrtkom American Express o vašim komunikacijama prema „korisnicima usluge kartičnog plaćanja“ American Express zahvaćenim podatkovnim incidentom (i pribavljanju 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 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, proglašom, 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.

Odjeljak 3 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 3. „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 3. „Obveze obeštećenja zbog „podatkovnog incidenta“](#)“.

Za „podatkovne incidente“ koji obuhvaćaju:

- 10.000 brojeva kartica American Express koji sadrže nešto od sljedećeg:
 - „osjetljivi podaci za provjeru autentičnosti“ ili
 - „datum isteka“
 tvrtku American Express ćete obeštetiti po cijeni od 5 USD po broju računa.

Međutim, American Express neće od vas zahtijevati obeštećenje za „podatkovne incidente“ koji obuhvaćaju:

- manje od 10.000 brojeva kartice American Express ili
- više od 10.000 brojeva kartice American Express, ako zadovoljite sljedeće uvjete:
 - obavijestili ste tvrtku American Express o „podatkovnom incidentu“ u skladu s [Odjeljak 3. „Obveze obeštećenja zbog „podatkovnog incidenta“](#),
 - bili ste u skladu 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 pokrivenih stranaka.

Bez obzira na prethodne članke ovog [Odjeljak 3. „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 100.000 USD po „podatkovnom incidentu“ (kako utvrđuje tvrtka American Express po vlastitoj procjeni) ako ne budete u skladu s obvezama navedenim u [Odjeljak 2. „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 100.000 USD.

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“) u skladu s ugovorom.

Ovdje navedene obveze „trgovca“ 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 vlastitoj procjeni može smanjiti obvezu za obeštećenjem za „trgovca“ samo 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 „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 kako slijedi:

Smanjenje obveze za obeštećenjem	Potrebni kriterij
Standardno smanjenje: 50 %	>75 % ukupnih transakcija obrađenih na „uređaju koji podržava čip“ ¹ ILI Tehnologija za izbjegavanje rizika koristi se na >75 % lokacija „trgovca“ ²

Smanjenje obveze za obeštećenjem	Potrebnii kriterij
Poboljšano smanjenje: 75 % do 100 %	>75 % svih transakcija obrađenih na „uređaju koji podržava čip“ 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 %) utvrđuje se na temelju manjeg postotka transakcija s pomoću „uređaja koji podržavaju čip“ i lokacija „trgovca“ na kojima se koristi druga „tehnologija za izbjegavanje rizika“. Primjeri u nastavku prikazuju 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. Na primjer, uporaba „uređaja koji podržava čip“ i obrada „kartica sa čipom“ kao transakcije s magnetskom trakom ili unosom ključa NIJE učinkovita uporaba te tehnologije.
- 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“.

Primjer	Uporaba tehnologije za izbjegavanje rizika	Jesu li ispunjeni uvjeti za smanjenje obveze za obeštećenjem?	Smanjenje
1	80 % ukupnih transakcija na „uređaju koji podržava čip“ 0 % lokacija koristi 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 % ukupnih transakcija na „uređaju koji podržava čip“ 77 % lokacija koristi drugu tehnologiju za izbjegavanje rizika	Da	77 % Poboljšano smanjenje (na temelju 77 % uporabe tehnologije za izbjegavanje rizika)
3	93 % ukupnih transakcija na „uređaju koji podržava čip“ 100 % lokacija koristi drugu tehnologiju za izbjegavanje rizika	Da	93 % Poboljšano smanjenje (na temelju 93 % transakcija na „uređajima koji podržavaju čip“)
4	40 % ukupnih transakcija na „uređaju koji podržava čip“ 90 % lokacija koristi drugu tehnologiju za izbjegavanje rizika	Ne	50 %: Standardno smanjenje (manje od 75 % transakcija na „uređajima koji podržavaju čip“ 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 4 Važna redovita provjera valjanosti vaših sustava

Trebate izvršiti sljedeće korake godišnje i tromjesečno 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 u okviru ovog pravilnika.

[Korak 2:](#) razumijevanje vaše razine i zahtjeva za „provjeru valjanosti“.

[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 razine 1“, „trgovci razine 2“ i svi „davatelji usluge“, kako je opisano u nastavku, moraju sudjelovati u programu sukladnosti tvrtke American Express u okviru ovog pravilnika navodeći ime i prezime, adresu e-pošte, broj telefona i fizičku poštansku adresu pojedinaca koji će postupati kao njihovi kontakti za sigurnost podataka. Te informacije morate poslati tvrtki SecureTrust, službi tvrtke Trustwave (<https://portal.securetrust.com>), koja upravlja programom u ime tvrtke American Express, i to na jedan od načina navedenih u [Korak 4: „Slanje dokumentacije za provjeru valjanosti“ tvrtki American Express](#) u nastavku. Tvrtku SecureTrust morate obavijestiti ako se te informacije promijene i posredovati ažurirane informacije kada je to primjenjivo. Ako ne dostavite kontakt informacije, to neće utjecati na naša prava na procjenu naknade za nesukladnost kao što je navedeno u [Tablica „Naknade za nesukladnost“](#).

Tvrtka American Express može po vlastitoj prosudbi zatražiti da određeni „trgovci“ razina 3 i 4 sudjeluju u programu sukladnosti tvrtke American Express u okviru ovog pravilnika tako da im pošalje pismenu obavijest. „Trgovac“ se mora uključiti ne kasnije od 90 dana od zaprimanja obavijesti.

Korak 2: Razumijevanje vaše razine i zahtjeva za „provjeru valjanosti“

S obzirom na količinu transakcija putem kartica American Express postoje četiri razine trgovaca i dvije razine davatelja usluge. Za „trgovce“ je to količina koju šalju njihove organizacije koja se proteže do najviše razine računa „trgovca“ za American Express.* Svrstat ćete se u jednu od razina specificiranih u tablicama za „trgovce“ i „davatelje usluge“ u nastavku. 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.

* To u slučaju „franšizodavaca“ uključuje količinu iz jedinica u njihovoj franšizi. „Franšizodavci“ koji svojim primateljima franšize nalažu primjenu specificiranog „sustava točke prodaje“ (Point of Sale, POS) ili „davatelji usluge“ također moraju pružiti „dokumentaciju za provjeru valjanosti“ za zahvaćene primatelje franšize.

Zahtjevi za „trgovce“

„Trgovci“ (ne „davatelji usluge“) imaju četiri moguće klasifikacije u vezi sa svojom razinom i zahtjevima za provjerom valjanosti. Nakon utvrđivanja razine „trgovca“ s popisa u nastavku pogledajte tablicu „Trgovac“ kako biste utvrdili zahtjeve za dokumentaciju za „provjeru valjanosti“:

- **„Trgovac razine 1“** – 2,5 milijuna ili više transakcija putem kartice American Express godišnje ili trgovac kojeg tvrtka American Express svojom odlukom svrsta u „trgovca razine 1“.
- **„Trgovac razine 2“** – od 50.000 do 2,5 milijuna „transakcija“ putem kartice American Express godišnje.
- **„Trgovac razine 3“** – od 10.000 do 50.000 „transakcija“ putem kartice American Express godišnje.
- **„Trgovac razine 4“** – manje od 10.000 „transakcija“ putem kartice American Express godišnje.

Tablica „Trgovac“

Razina trgovca/ broj American Express transakcija godišnje	Dokumentacija za provjeru valjanosti		
	Procjena na lokaciji s izvješćem o sukladnosti (ROC)	Upitnik za samoprocjenu (SAQ) i tromjesečno skeniranje mreže	Ovjera programa STEP za prikladne trgovce
Razina 1/ 2,5 milijuna ili više	Obvezno	Nije primjenjivo	Opcija (zamjenjuje ROC)
Razina 2/ 50.000 do 2,5 milijuna	Opcija	SAQ obavezan (osim ako se ne dostavlja procjena na lokaciji). Skeniranje obvezno s određenim kategorijama SAQ-a	Opcija (zamjenjuje SAQ i skeniranje mreže ili ROC)
Razina 3/ 10.000 do 50.000	Opcija	SAQ je opcija (obavezan ako to zahtijeva American Express). Skeniranje obvezno s određenim kategorijama SAQ-a	Opcija (zamjenjuje SAQ i skeniranje mreže ili ROC)
Razina 4/ 10.000 ili manje	Opcija	SAQ je opcija (obavezan ako to zahtijeva American Express). Skeniranje obvezno s određenim kategorijama SAQ-a	Opcija (zamjenjuje SAQ i skeniranje mreže ili ROC)

* Radi otklanjanja sumnje, „trgovci“ razina 3 i 4 ne trebaju slati „dokumentaciju za provjeru valjanosti“ osim ako to ne zatraži tvrtka American Express po vlastitoj procjeni, ali svakako moraju biti sukladni i odgovorni u pogledu svih drugih odredbi ovog radnog pravilnika za sigurnost podataka.

Tvrtka American Express po potrebi može provjeriti točnost i prikladnost dostavljene PCI dokumentacije za provjeru valjanosti te angažirati „kvalificiranog procjenitelja sigurnosti“ (QSA) ili „forenzičara za PCI“ (PFI) po vlastitom izboru.

Program za unaprjeđenje sigurnosne tehnologije (STEP)

„Trgovci“ koji su sukladni s PCI DSS-om moraju, ako American Express tako odluči, ispunjavati i uvjete STEP-a (Security Technology Enhancement Programme) 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 na sljedeće načine:

- **EMV** – na aktivnom „uređaju koji podržava čip“ s valjanim i trenutačnim EMVCo (www.emvco.com) odobrenjem/certifikatom i koji može obrađivati „transakcije“ s „karticama sa čipom“ u skladu s AEIPS-om. („Trgovci“ u SAD-u moraju uključivati beskontaktnu „transakciju“)
- **„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“

„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.

Zahtjevi za „davatelje usluge“

„Davatelji usluge“ (ne „trgovci“) imaju dvije moguće klasifikacije u vezi sa svojom razinom i zahtjevima za ovjerom valjanosti. Nakon utvrđivanja razine „davatelja usluge“ s popisa u nastavku pogledajte tablicu „Davatelj usluge“ kako biste utvrdili zahtjeve za dokumentaciju za provjeru valjanosti.

„Davatelj usluge razine 1“ – 2,5 milijuna ili više „transakcija“ putem kartice American Express na godinu ili „davatelj usluge“ 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 usluge“ koje tvrtka American Express ne smatra „davateljima usluge razine 1“.

„Davatelji usluge“ ne zadovoljavaju uvjete za STEP.

Tablica „Davatelj usluge“

Razina	Dokumentacija za provjeru valjanosti	Zahtjev
1	Godišnja procjena sigurnosti na lokaciji o sukladnosti	Obvezno
2	Godišnji SAQ D (davatelj usluge) i tromjesečno skeniranje mreže ILI godišnje izvješće o procjeni sigurnosti na lokaciji, po želji.	Obvezno

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

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 tablicama „Trgovac“ i „Davatelj usluge“ gore.

Godišnja procjena sigurnosti na lokaciji – godišnja procjena sigurnosti na lokaciji podroban je pregled na lokaciji vaše opreme, sustava i mreža (i njihovih komponenti) na kojima se spremaju, obrađuju ili prenose „podaci vlasnika kartica“ ili „osjetljivi podaci za provjeru autentičnosti“. Postupak treba provesti:

- QSA ili
- vi i mora ga potvrditi vaš izvršni voditelj, glavni financijski voditelj, glavni voditelj za informacijsku sigurnost ili ravnatelj i trebate ga jednom godišnje poslati tvrtki American Express na primjenjivoj „ovjeri sukladnosti“ (Attestation of Compliance, AOC).

AOC mora potvrditi sukladnost sa svim zahtjevima PCI DSS-a i na zahtjev uključiti kopije cjelovitog izvješća o sukladnosti („trgovci“ i „davatelji usluge razine 1“).

Godišnji „upitnik za samoprocjenu“ – godišnji „upitnik za samoprocjenu“ postupak je u kojem se koristi PCI DSS SAQ (SAQ) koji omogućuje samostalan pregled vaše opreme, sustava i mreža (i njihovih komponenti) na kojima se spremaju, obrađuju ili prenose podaci vlasnika kartica ili „osjetljivi podaci za provjeru autentičnosti“. Morate ga vi provesti i mora ga certificirati vaš izvršni voditelj, glavni financijski voditelj, glavni voditelj za informacijsku sigurnost ili ravnatelj. Odjeljak AOC upitnika SAQ treba godišnje slati tvrtki American Express. Odjeljak AOC upitnika SAQ mora certificirati vašu sukladnost sa svim zahtjevima PCI DSS i uključivati cjelovite kopije upitnika SAQ na zahtjev („trgovci razina“ 2, 3 i 4 te „davatelji usluge razine 2“).

Tromjesečno skeniranje mreže – tromjesečno skeniranje mreže postupak je daljinskog testiranja vaših računalnih mreža i web poslužitelja povezanih s internetom radi pronalaženja mogućih nedostataka i ranjivosti. To treba izvršiti „odobreni skeniratelj“ (Approved Scanning Vendor, **ASV**). Morate ispuniti i tvrtki American Express poslati ASV izvješće o skeniranju za „ovjeru sukladnosti skeniranja“ (Attestation of Scan Compliance, **AOSC**) ili izvršni sažetak nalaza skeniranja (i na zahtjev kopije cjelovitog skeniranja). AOSC ili izvršni sažetak mora potvrditi da rezultati zadovoljavaju postupke PCI DSS skeniranja, da nisu identificirani vrlo rizični problemi te da je skeniranje prolazno ili sukladno (svi „trgovci“ osim onih koji dostavljaju i izvješće o procjeni sigurnosti na lokaciji, trgovci koji zadovoljavaju uvjete programa STEP i svi davatelji usluge). Kako bi se izbjegle nedoumice, tromjesečno skeniranje mreže obvezno je ako je to zahtjev primjenjivog upitnika SAQ.

Dokumentacija za godišnju provjeru valjanosti programa STEP – godišnja ovjera kvalifikacije programa STEP za American Express („ovjera programa STEP“) dostupna je samo za „trgovce“ koji zadovoljavaju uvjete navedene u [Korak 2: „Razumijevanje vaše razine i zahtjeva za „provjeru valjanosti““](#) gore. Ovjera programa STEP uključuje postupak je u kojem se koristi PCI DSS koji omogućuje samostalan pregled vaše opreme, sustava i mreža (i njihovih komponenti) na kojima se spremanju, obrađuju ili prenose podaci vlasnika kartica ili „osjetljivi podaci za provjeru autentičnosti“ (ili oboje). Morate ga vi provesti i mora ga certificirati vaš izvršni voditelj, glavni

financijski voditelj, glavni voditelj za informacijsku sigurnost ili ravnatelj. Morate dovršiti postupak godišnjim slanjem obrasca za ovjeru programa STEP tvrtki American Express. (Samo za „trgovce“ koji zadovoljavaju uvjete programa STEP). Predložak obrasca za godišnju ovjeru programa STEP dostupan je za preuzimanje putem sigurnog portala tvrtke SecureTrust.

„Sažetak sukladnosti“ (Summary of Compliance, SOC) – SOC je dokument putem kojeg „franšizodavac“ ili „davalatelj usluge“ može poslati izvješće o statusu PCI sukladnosti svojih primatelja franšiza. Predložak SOC-a dostupan je za preuzimanje putem sigurnog portala tvrtke SecureTrust.

Nesukladnost s PCI DSS-om – ako niste sukladni s PCI DSS-om, morate dostaviti jedan od sljedećih dokumenata:

- ovjeru sukladnosti (AOC), uključujući i „dio 4. Akcijski plan za status nesukladnosti“
- PCI sažetak alata za utvrđivanje prioriteta s ovjerom sukladnosti (PASAOC)
- predložak projektnog plana (dostupan je za preuzimanje putem sigurnog portala tvrtke SecureTrust)

U svakom od navedenih dokumenata mora biti utvrđen rok za otklanjanje problema, koji, ako se želi postići sukladnost, ne smije biti duži od 12 mjeseci od sastavljanja dokumenata. Odgovarajući dokument morate poslati tvrtki American Express na jedan od načina navedenih u [Korak 4: „Slanje „dokumentacije za provjeru valjanosti“ tvrtki American Express“](#) u nastavku. Tvrtku American Express morate povremeno obavještavati o napretku u otklanjanju statusa nesukladnosti (trgovci razina 1, 2, 3 i 4, te svi davatelji usluge). Radi otklanjanja svake sumnje, „trgovci“ koji nisu sukladni s PCI DSS-om ne ispunjavaju uvjete za STEP. Tvrtka American Express neće vam nametati naknade koje nisu povezane s ovjerom (opisano u nastavku) prije datuma za otklanjanje problema, ali ćete i dalje biti odgovorni tvrtki American Express u pogledu svih obveza za obeštećenjem za „podatkovni incident“ i morat ćete poštivati sve druge odredbe iz ovog pravilnika.

Korak 4: Slanje „dokumentacije za provjeru valjanosti“ tvrtki American Express

Svi trgovci i davatelji usluge koji moraju sudjelovati u programu sukladnosti tvrtke American Express moraju poslati dokumentaciju za provjeru valjanosti koja je u tablicama u [Korak 2: „Razumijevanje vaše razine i zahtjeva za „provjeru valjanosti““](#) označena kao „obavezna“. Svoju „dokumentaciju za provjeru valjanosti“ morate poslati tvrtki SecureTrust na jedan od sljedećih načina:

- **Sigurni portal:** „Dokumentaciju za provjeru valjanosti“ možete prenijeti putem sigurnog portala tvrtke SecureTrust na <https://portal.securetrust.com>.
Kontaktirajte tvrtku SecureTrust na telefonski broj za vašu zemlju ili putem e-pošte na americanexpresscompliance@securetrust.com za upute za uporabu tog portala.
- **Sigurni faks:** „Dokumentaciju za provjeru valjanosti“ možete faksirati na: +1 (312) 276-4019. (+ označava prefiks za izravno međunarodno biranje „IDD“, naplaćuje se naknada za međunarodne pozive).
Navedite svoje ime, DBA (poslovanje kao) naziv, ime kontakta za sigurnost podataka, adresu i broj telefona te, samo za „trgovce“, 10-znamenkasti broj „trgovca“ American Express.

U slučaju općenitih pitanja o programu ili postupku opisanom gore obratite se tvrtki SecureTrust na + 800 9000 1140 ili +1 (312) 267-3208 ili putem e-pošte na americanexpresscompliance@securetrust.com.

Sukladnost i ovjera vrše se o vašem trošku. Slanjem „dokumentacije za provjeru valjanosti“ tvrtki American Express izjavljujete i jamčite da imate ovlasti za otkrivanje sadržanih informacija i da tvrtki American Express pružate „dokumentaciju za provjeru valjanosti“ bez kršenja prava bilo koje druge stranke.

Tržišta	Telefonski broj SecureTrust
Argentina	+ 800 9000 1140
Australija	+ 800 9000 1140
Austrija	+ 800 9000 1140
Bugarska	+ 312 267 3208
Češka	+ 800 144 316
Cipar	+ 800 9000 1140
Danska	+ 800 9000 1140
Estonija	+ 312 267 3208
Francuska	+ 800 9000 1140
Grčka	+ 312 267 3208
Hong Kong	+ 800 9000 1140
Hrvatska	+ 312 267 3208
IDC	+ 888 900 0114
Indija	+ 800 9000 1140
Irska	+ 800 9000 1140
Island	+ 800 9000 1140
Italija	+ 800 9000 1140
Japan	+ 312 267 3208
Kanada	1 866 659 9016
Latvija	+ 312 267 3208
Litva	+ 312 267 3208

Tržišta	Telefonski broj SecureTrust
Mađarska	+ 800 9000 1140
Malta	+ 312 267 3208
Meksiko	+ 888 900 0114
Nizozemska	+ 312 267 3208
Njemačka	+ 800 9000 1140
Norveška	+ 800 9000 1140
Novi Zeland	+ 800 9000 1140
Poljska	+ 800 9000 1140
Portugal	+ 312 267 3208
Rumunjska	+ 312 267 3208
Rusija	+ 312 267 3208
Singapur	+ 800 9000 1140
Sjedinjene Američke Države	1 866 659 9016
Slovačka	+ 312 267 3208
Slovenija	+ 312 267 3208
Španjolska	+ 800 9000 1140
Švedska	+ 800 9000 1140
Tajland	+ 800 9000 1140
Tajvan	+ 312 267 3208
Ujedinjeno Kraljevstvo	+ 800 9000 1140

+ označava prefiks za izravno međunarodno biranje „IDD“, naplaćuje se naknada za međunarodne pozive

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 važećeg roka. Tvrtka American Express posebno će vas obavijestiti o važećem roku za svako godišnje i tromjesečno razdoblje.

Pošaljite dokumentaciju tvrtki American Express do važećeg roka. Tvrtka American Express posebno će vas obavijestiti o važećem roku za svako godišnje i tromjesečno razdoblje. U nastavku pogledajte tablicu „Naknade za nesukladnost“ za važeće naknade u vašoj zemlji.

Opis	Trgovac ili davatelj usluge razine 1	Trgovac ili davatelj usluge razine 2, trgovac STEP	Trgovac razine 3 ili 4
Naknada za nesukladnost procijenit će se ako se „dokumentacija za provjeru valjanosti“ ne zaprimi do prvog roka.	Naknada za prvi mjesec za razinu 1	Naknada za prvi mjesec za razinu 2	Mjesečna naknada
Dodatna naknada za nesukladnost procijenit će se ako se „dokumentacija za provjeru valjanosti“ ne zaprimi u roku od 30 dana od prvog roka.	Naknada za drugi mjesec za razinu 1	Naknada za drugi mjesec za razinu 2	
Dodatna naknada za nesukladnost procijenit će se ako se „dokumentacija za provjeru valjanosti“ ne zaprimi u roku od 60 dana od prvog roka.	Naknada za treći mjesec za razinu 1	Naknada za treći mjesec za razinu 3	

Ako tvrtka American Express ne zaprimi vašu obveznu „dokumentaciju za provjeru valjanosti“ u roku od 60 dana od prvog roka, tada tvrtka American Express ima pravo na raskidanje ugovora u skladu s njegovim odredbama kao i na kumulativnu naplatu tekućih naknada za nesukladnost.

Tablica „Naknade za nesukladnost“

Tržište	Razina	Vrsta	Valuta	Naknada za prvi mjesec	Naknada za drugi mjesec	Naknada za treći mjesec
Australija	Razina 1	Trgovac ili davatelj usluge	AUD	35.000	49.000	63.000
	Razina 2	Trgovac ili davatelj usluge	AUD	7.000	14.000	21.000
	Razina 3 i 4	Trgovac	AUD	Mjesečna naknada: 20		
Bugarska	Razina 1	Trgovac ili davatelj usluge	BGN	28.000	40.000	51.000
	Razina 2	Trgovac ili davatelj usluge	BGN	5.500	11.000	16.500
	Razina 3 i 4	Trgovac	BGN	Mjesečna naknada: 33		
Hrvatska	Razina 1	Trgovac ili davatelj usluge	HRK	105.000	152.000	195.000
	Razina 2	Trgovac ili davatelj usluge	HRK	21.000	42.000	63.000
	Razina 3 i 4	Trgovac	HRK	Mjesečna naknada: 130		

Tržište	Razina	Vrsta	Valuta	Naknada za prvi mjesec	Naknada za drugi mjesec	Naknada za treći mjesec
Cipar, Estonija, Francuska, Njemačka, Irska, Španjolska, Latvija, Litva, Portugal, Slovačka, Slovenija	Razina 1	Trgovac ili davatelj usluge	EUR	19.000	26.000	34.000
	Razina 2	Trgovac ili davatelj usluge	EUR	4.000	7.500	11.000
	Razina 3 i 4	Trgovac	EUR	Mjesečna naknada: 15		
Češka	Razina 1	Trgovac ili davatelj usluge	CZK	392.000	564.000	721.000
	Razina 2	Trgovac ili davatelj usluge	CZK	78.300	157.000	235.000
	Razina 3 i 4	Trgovac	CZK	Mjesečna naknada: 440		
Danska	Razina 1	Trgovac ili davatelj usluge	DKK	110.000	156.000	200.000
	Razina 2	Trgovac ili davatelj usluge	DKK	22.000	42.000	65.000
	Razina 3 i 4	Trgovac	DKK	Mjesečna naknada: 130		
Hong Kong	Razina 1	Trgovac ili davatelj usluge	HKD	25.000	35.000	45.000
	Razina 2	Trgovac ili davatelj usluge	HKD	5.000	10.000	15.000
	Razina 3 i 4	Trgovac	HKD	Mjesečna naknada: 150		
Mađarska	Razina 1	Trgovac ili davatelj usluge	HUF	4.650.000	6.700.000	8.600.000
	Razina 2	Trgovac ili davatelj usluge	HUF	930.000	1.860.000	2.800.000
	Razina 3 i 4	Trgovac	HUF	Mjesečna naknada: 5.500		
Island	Razina 1	Trgovac ili davatelj usluge	ISK	3.070.000	4.300.000	5.500.000
	Razina 2	Trgovac ili davatelj usluge	ISK	615.000	920.000	1.227.200
	Razina 3 i 4	Trgovac	ISK	Mjesečna naknada: 2.400		

Tržište	Razina	Vrsta	Valuta	Naknada za prvi mjesec	Naknada za drugi mjesec	Naknada za treći mjesec
Novi Zeland	Razina 1	Trgovac ili davatelj usluge	NZD	35.000	49.000	63.000
	Razina 2	Trgovac ili davatelj usluge	NZD	7.000	14.000	21.000
	Razina 3 i 4	Trgovac	NZD	Mjesečna naknada: 20		
Norveška	Razina 1	Trgovac ili davatelj usluge	NOK	135.000	195.000	249.000
	Razina 2	Trgovac ili davatelj usluge	NOK	27.000	54.000	81.000
	Razina 3 i 4	Trgovac	NOK	Mjesečna naknada: 170		
Singapur	Razina 1	Trgovac ili davatelj usluge	SGD	38.000	53.000	68.000
	Razina 2	Trgovac ili davatelj usluge	SGD	7.500	15.000	22.500
	Razina 3 i 4	Trgovac	SGD	Mjesečna naknada: 25		
Švedska	Razina 1	Trgovac ili davatelj usluge	SEK	175.000	245.000	315.000
	Razina 2	Trgovac ili davatelj usluge	SEK	35.000	70.000	105.000
	Razina 3 i 4	Trgovac	SEK	Mjesečna naknada: 135		
Ujedinjeno Kraljevstvo	Razina 1	Trgovac ili davatelj usluge	GBP	12.500	18.000	23.000
	Razina 2	Trgovac ili davatelj usluge	GBP	2.500	5.000	7.500
	Razina 3 i 4	Trgovac	GBP	Mjesečna naknada: 15		

Odjeljak 5 Povjerljivost

Tvrtka American Express poduzet će razumne mjere da vaša izvješća o sukladnosti, uključujući „dokumentaciju za provjeru valjanosti“ zadrže (što vrijedi i za njihove predstavnike i podugovorene stranke, uključujući tvrtku SecureTrust) povjerljivima i „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 bez obveze za povjerljivošću,

- d. koju je neovisno razvila tvrtka American Express ili,
- e. 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 6 Ograda 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.

Korisna web-mjesta

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

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

Pojmovnik

Za svrhu ovog [Radni pravilnik za sigurnost podataka \(DSOP\)](#) primjenjuju se sljedeće definicije i provjera u slučaju nepodudarnosti s pojmovima koji se nalaze u *Propisi za trgovce*.

Aplikacija za plaćanje ima značenje kako je navedeno u rječniku pojmova za aplikaciju za plaćanje u standardu za sigurnost podataka u industriji platnih kartica koji je dostupan na www.pcisecuritystandards.org.

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 izdavateljima 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.

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 dobivenim 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.

Franšizodavac 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 d primatelja franšize zahtijeva plaćanje naknade.

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 izdavatelj 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 računa. 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.

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

Naplata se odnosi na plaćanje izvršeno karticom.

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.

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

Osjetljivi podaci za provjeru autentičnosti imaju značenje navedeno u trenutačnom pojmovniku PCI DSS-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.

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 koji je odobrilo 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 „aplikaciju 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 vlasnika kartice ima značenje navedeno u trenutačnom pojmovniku PCI DSS-a.

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 (card identification number, CID).

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 čijom uporabom upravljate,
- 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).

Pokrivene stranke odnosi se na sve vaše zaposlenike, agente, predstavnike, podugovaratelje, procesore, davatelje usluge, dobavljače vaše opreme na točki prodaje (POS) ili POS sustave ili rješenja za obradu plaćanja, subjekte povezane s vašim trgovačkim računom American Express i sve druge stranke kojima možete posredovati pristup podacima o korisniku usluge kartičnog plaćanja u skladu s ugovorom.

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

Program za unaprjeđenje sigurnosne tehnologije (Security Technology Enhancement Program, STEP) odnosi se na program tvrtke American Express kojim se trgovci potiču na razvoj tehnologija koje unaprjeđuju sigurnost podataka. Kako bi zadovoljili uvjete za program STEP, trgovci ne smiju imati podatkovni incident u proteklih 12 mjeseci prije slanja godišnje ovjere za program STEP i moraju vršiti najmanje 75 % svih transakcija putem šifriranja od točke do točke ili osobnih transakcija putem EMV uređaja koji podržavaju čip.

Sažetak sukladnosti (SOC) odnosi se na PCI dokument za provjeru valjanosti koji koristi franšizodavac za iskazivanje PCI statusa sukladnosti svojih zahvaćenih primatelja franšize.

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

Sustav točaka prodaje (Point of Sale, 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.

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.

Tehnologija za izbjegavanje rizika odnosi se na tehnološka rješenja koja unaprjeđuju 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: EMV, šifriranje od točke do točke i tokenizacija.

Transakcija se odnosi na naplatu ili kredit izvršen putem kartice.

Transakcije koje pokreće kupac (BIP) odnosi se na platne transakcije koje omogućuje datoteka s uputama za plaćanje koja se obrađuje putem BIP-a.

Trgovac se odnosi na trgovca i sve njegove pridružene tvrtke koje prihvaćaju karticu American Express u skladu s ugovorom s tvrtkom American Express i 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 2,5 milijuna transakcija putem kartice American Express godišnje.

„**Trgovac razine 3**“ odnosi se na „trgovca“ s 10.000 do 50.000 transakcija putem kartice American Express godišnje.

„**Trgovac razine 4**“ odnosi se na „trgovca“ s manje od 10.0000 transakcija putem kartice American Express godišnje.

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 čip 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 rječniku pojmova 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.

Vremenski okvir podatkovnog incidenta odnosi se na razdoblje koje počinje s datumom kompromitiranja, ako je poznat, ili 365 dana prije datuma obavijesti ako stvarni datum kompromitiranja nije poznat. Vremenski okvir podatkovnog incidenta završava 30 dana nakon datuma obavijesti.

Zahtjevi Payment Card Industry Security Standards Council, LLC (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.