AMERICAN EXPRESS

Datu drošības darbības politika (DSOP)

Kā līderim patērētāju aizsardzības jomā uzņēmumam American Express ir ilgtermiņa apņemšanās aizsargāt Kartes Lietotāja Informāciju un Sensitīvos Autentifikācijas Datus, nodrošinot to drošu glabāšanu.

Apdraudēti dati negatīvi ietekmē patērētājus, Tirgotājus, Pakalpojumu sniedzējus un karšu izdevējus. Pat viens incidents var nodarīt nopietnu kaitējumu uzņēmuma reputācijai un mazināt tā spēju efektīvi veikt komercdarbību. Šo draudu novēršana, īstenojot drošības darbības politiku, var palīdzēt vairot klientu uzticību, palielināt rentabilitāti un uzlabot uzņēmuma reputāciju.

American Express zina, ka arī mūsu Tirgotāji un Pakalpojumu sniedzēji (kopīgi **jūs**) ir nobažījušies par to un pieprasa, lai jūs, pildot savus pienākumus, ievērotu datu drošības noteikumus savā līgumā par American Express® Kartes pieņemšanu (Tirgotāju gadījumā) vai apstrādāšanu (Pakalpojumu sniedzēju gadījumā) (katrs attiecīgi **Līgums**) un šo *Datu drošības darbības politiku*, kuru mēs laiku pa laikam varam grozīt. Šīs prasības attiecas uz visām jūsu iekārtām, sistēmām un tīkliem (un to komponentiem), kur tiek glabātas, apstrādātas vai pārraidītas Šifrēšanas atslēgas, Kartes lietotāja dati vai Sensitīvie autentifikācijas dati (vai to kombinācija).

Ar lielo sākuma burtu rakstītajiem terminiem, kuri šeit lietoti, bet nav definēti, ir šīs politikas beigās terminu sarakstā sniegtā nozīme.

Sadaļa 1 Šifrēšanas atslēgu, Kartes lietotāja datu un Sensitīvo autentifikācijas datu aizsardzības standarti

Jums ir jāveic un jāliek veikt jūsu Aptvertajām personām turpmāk minētais:

- jāuzglabā Kartes lietotāja dati vienīgi ar nolūku veicināt American Express Kartes darījumus saskaņā ar Līgumu un atbilstoši Līguma prasībām.
- jāievēro spēkā esošās Maksājumu Karšu Nozares Datu Drošības Standarta (PCI DSS) un citas Maksājumu Karšu Nozares Drošības Standartu Padomes (PCI SSC) prasības, kas attiecināmas uz jūsu veikto Kartes lietotāja datu vai Sensitīvo autentifikācijas datu apstrādi, uzglabāšanu vai pārsūtīšanu, ne vēlāk kā šīs piemērojamās prasības versijas īstenošanas spēkā stāšanās datumā.
- izmantojot jaunās vai nomainītās PIN ievades ierīces vai maksājumu pieteikumus (vai abus), apmeklētajās vietās jāizmanto vienīgi PCI Apstiprinātās ierīces vai pieteikumi.

Jums ir jāaizsargā visi American Express Maksājuma Ieraksti un Kredīta Ieraksti, kas tiek saglabāti saskaņā ar Līgumu atbilstoši šiem datu drošības noteikumiem; jums ir jāizmanto šie ieraksti vienīgi Līguma mērķiem un atbilstoši jāaizsargā tie. Jūs uzņematies finansiālu un cita veida atbildību pret American Express par to, lai nodrošinātu, ka jūsu Aptvertās Personas ievēro šos datu drošības noteikumus (izņemot nolūku pierādīt, ka jūsu Aptvertās Personas ievēro šo politiku saskaņā ar zemāk esošo Sadaļa 4, „Svarīga periodiska jūsu sistēmu validācija“, ja vien šajā sadaļā nav noteikts citādi.)

Sadaļa 2 Datu incidentu pārvaldības pienākumi

Jums nekavējoties un nekādā gadījumā ne vēlāk kā divdesmit četras (24) stundas pēc Datu Incidenta atklāšanas ir jāinformē par to American Express.

Lai informētu American Express, lūdzu, sazinieties ar American Express Uzņēmumu Incidentu Reaģēšanas Programmu [Enterprise Incident Response Programme] (*EIRP*) pa tālruni +1 (602) 537-3021 (+ norāda starptautiskā tiešā numura „IDD" prefiksu, piemēro starptautiskā zvana tarifu), vai izmantojot e-pasta adresi EIRP@aexp.com. Jums ir jānorāda jūsu kontaktpersona saistībā ar šādu Datu incidentu. Papildus tam:

- Jums jāveic katra Datu aizsardzības pārkāpuma rūpīga izmeklēšana.
- Datu aizsardzības pārkāpuma gadījumā, kas skar 10 000 vai vairāk unikālo Karšu kontu numuru, jums ir jāpiesaista PCI (PFI) Izmeklētājs izmeklēšanas veikšanai piecu (5) dienu laikā pēc šāda Datu incidenta atklāšanas.
- Nerediģēts izmeklēšanas ziņojums jāiesniedz American Express desmit (10) darba dienu laikā pēc izmeklēšanas pabeigšanas.
- Jums ir nekavējoties jānorāda American Express visi Apdraudēto karšu numuri. American Express patur tiesības veikt iekšējo analīzi, lai identificētu Datu incidentā iesaistīto Karšu numurus.

Izmeklēšanas ziņojumi jāveic, izmantojot pašlaik PCI pieejamo Izmeklēšanas incidenta galīgā ziņojuma veidni. Šādā ziņojumā ir jāietver izmeklēšanas pārskati, atbilstības ziņojumi un visa pārējā informācija, kas saistīta ar Datu incidentu; jāidentificē Datu incidenta iemesls; jāapstiprina, vai Datu aizsardzības pārkāpuma brīdī jūs ievērojāt PCI DSS; un jāapliecina jūsu spēja novērst turpmākos Datu incidentus (i) iesniedzot plānu visu PCI DSS trūkumu novēršanai un (ii) piedaloties American Express atbilstības programmā (kā minēts tālāk). Pēc American Express pieprasījuma jums ir jāiesniedz Kvalificēta drošības vērtētāja (QSA) apliecinājums, ka nepilnības ir novērstas.

Neskatoties uz šīs Sadaļa 2, „Datu incidentu pārvaldības pienākumi" iepriekšējiem punktiem:

- American Express var pēc saviem ieskatiem pieprasīt jums iesaistīt PFI, lai veiktu tādu Datu incidentu izmeklēšanu, kuros iesaistīti vairāk kā 10 000 unikālo Karšu numuru. Visām šādām izmeklēšanām ir jāatbilst prasībām, kas noteiktas iepriekš šajā Sadaļa 2, „Datu incidentu pārvaldības pienākumi", un tās ir jāveic American Express pieprasītajā termiņā.
- American Express var pēc saviem ieskatiem atsevišķi iesaistīt PFI, lai tas veiktu jebkura Datu incidenta izmeklēšanu, un var prasīt jums segt šādas izmeklēšanas izmaksas.

Jūs piekrītat sadarboties ar American Express, lai izlabotu visas problēmas, kas izriet no Datu incidenta, tostarp konsultēties ar American Express par jūsu saziņu ar Karšu lietotājiem, ko skāris Datu incidents, un sniegt (un saņemt visus atteikumus, kas nepieciešami, lai sniegtu) American Express visu attiecīgo informāciju, lai pārbaudītu jūsu spēku novērst turpmākus Datu incidentus Līgumam atbilstošā veidā.

Neskatoties uz Līgumā norādītiem citiem pretējiem konfidencialitātes ievērošanas pienākumiem, American Express ir tiesības atklāt informāciju par Datu incidentu American Express Karšu lietotājiem, citiem American Express tīkla dalībniekiem un sabiedrībai saskaņā ar Amerikas tiesību aktu prasībām; tiesas, administratīviem vai regulēšanas rīkojumu, dekrētu, pavēsti, pieprasījumu vai citu procesu; lai mazinātu krāpšanas vai cita kaitērjuma risku; vai citādi tādā mērā, kas ir piemērots, lai nodrošinātu American Express tīkla darbību.

Sadaļa 3 Pienākums atlīdzināt zaudējumus par Datu incidentu

Jūsu Līgumā paredzētās saistības atlīdzināt uzņēmumam American Express zaudējumus par Datu Incidentiem tiek noteiktas, neatsakoties no jebkādām citām American Express tiesībām un tiesiskās aizsardzības līdzekļiem, saskaņā ar šo Sadaļa 3, „Pienākums atlīdzināt zaudējumus par Datu incidentu“. Papildus pienākumam atlīdzināt zaudējumus (ja tādi ir) jums var būt jāmaksā Datu incidenta neatbilstības maksa, ka aprakstīta turpmāk tekstā šajā Sadaļa 3, „Pienākums atlīdzināt zaudējumus par Datu incidentu“.

Par Datu incidentiem, kuros iesaistīts:

- 10 000 vai vairāk American Express Karšu numuri ar vienu no šeit norādītajiem:
  - Sensitīviem autentifikācijas datiem vai
  - Derīguma termiņu

  jūs maksājat kompensāciju American Express saskaņā ar likmi $5 USD par vienu konta numuru.

Taču American Express nepieprasīs no jums kompensāciju par Datu incidentu, kurā iesaistīts:

- mazāk kā 10 000 American Express karšu numuru vai
- vairāk kā 10 000 American Express karšu numuru, ja jūs izpildāt šādus nosacījumus:
  - jūs ziņojāt American Express par Datu incidentu saskaņā ar šo Sadaļa 3, „Pienākums atlīdzināt zaudējumus par Datu incidentu“,
  - Datu incidenta brīdī jūs ievērojāt PCI DSS (kas konstatēts Datu incidenta PFI izmeklēšanā), un
  - Datu incidentu neizraisīja jūsu vai jūsu Aptverto personu nepareiza rīcība.

Neskatoties uz šīs Sadaļa 3, „Pienākums atlīdzināt zaudējumus par Datu incidentu“ iepriekšējiem punktiem, par katru Datu incidentu neatkarīgi no American Express Karšu skaita jūs maksājat American Express Datu incidenta neatbilstības maksu, kas nepārsniedz $100 000 USD par Datu incidentu (ko pēc saviem ieskatiem nosaka American Express), ja jūs neizpildat kādu no saviem pienākumiem, kas noteikti Sadaļa 2, „Datu incidentu pārvaldības pienākumi“. Lai izvairītos no šaubām, kopējā maksa par Datu incidenta neatbilstības maksu, kas aprēķināta par jebkuru atsevišķu Datu incidentu, nedrīkst pārsniegt $100 000 USD.

American Express izslēgs no saviem aprēķiniem jebkuru American Express Kartes konta numuru, kas bija iesaistīts iepriekšējā Datu incidenta kompensācijas prasībā, kas ticis iesniegts divpadsmit (12) mēnešu laikā pirms Paziņošanas datuma. Visi saskaņā ar šo metodiku veiktie American Express aprēķini ir galīgi.

American Express var izsniegt jums rēķinu par pilnu jūsu kompensācijas saistību par Datu incidentiem summu vai atskaitīt šo summu no American Express maksājumiem jums (vai attiecīgi debetēt jūsu bankas Kontu) saskaņā ar Līgumu.

Tirgotāju saistības atlīdzināt zaudējumus par Datu incidentiem saskaņā ar šo neuzskata par nejaušiem, netiešiem, spekulatīviem, izrietošiem, īpašiem, soda vai parauga zaudējumu atlīdzības gadījumiem ar nosacījumu, ka šādas saistības neietver zaudējumus, kas saistīti ar peļņas vai ienākumu zaudējumu, nemateriālās vērtības zaudējumu vai komercdarbības iespēju zaudējumu.

American Express pēc saviem ieskatiem ir tiesības samazināt zaudējumu atlīdzību Tirgotājiem tikai par Datu incidentiem, kas atbilst šādiem kritērijiem:

- pirms Datu incidenta un visa Datu incidenta gadījumu loga laikā tika izmantotas attiecināmās Risku mazināšanas tehnoloģijas;
- ir pabeigta rūpīga izmeklēšana saskaņā ar PFI programmu (ja nav citas iepriekšējas rakstiskas vienošanās);
- izmeklēšanas ziņojumā ir skaidri norādīts, ka Risku mazināšanas tehnoloģijas tika izmantotas, lai apstrādātu, glabātu un/vai sūtītu datus Datu incidenta laikā; un
- jūs neglabājāt (tostarp visā Datu incidenta gadījumu loga laikā) Sensitīvus autentifikācijas datus vai jebkurus Kartes Lietotāja Datus, kas nav padarīti neizlasāmi.

Ja ir piemērojama zaudējumu atlīdzināšanas pienākuma apmēra samazināšana, tad jūsu zaudējumu atlīdzināšanas pienākuma apmērs (atskaitot jebkādas maksājamās neatbilstības maksas) tiek samazināts atbilstoši zemāk norādītajam:

Zaudējumu atlīdzības saistību samazināšana	Nepieciešamie kritēriji
Standarta samazinājums: 50%	>75% no kopējo Darījumu skaita apstrādāti ar Mikroshēmas ierīcēm[1] VAI
	Riska mazināšanas tehnoloģija tiek izmantota >75% Tirgotāja atrašanās vietu[2]
Paaugstināts samazinājums: 75% līdz 100%	>75% no kopējo Darījumu skaita apstrādāti ar Mikroshēmas ierīcēm[1] UN cita Riska mazināšanas tehnoloģija izmantota >75% Tirgotāja atrašanās vietu[2]

[1] Noteikts American Express iekšējā analīzē

[2] Noteikts PFI izmeklēšanā

- Palielinātais samazinājums (no 75% līdz 100%) tiek noteikts, ņemot vērā mazāko no to Darījumu apmēru, kuros tiek izmantotas ar Mikroshēmas ierīces, UN Tirgotāju vietas, kurās tiek izmantotas citas Risku mazināšanas tehnoloģijas. Tālāk minētie piemēri ilustrē zaudējumu atlīdzināšanas pienākuma samazinājuma aprēķinu.
- Lai kvalificētu tehnoloģiju kā Risku mazināšanas tehnoloģiju, jums jādemonstrē efektīva tehnoloģijas izmantošana atbilstoši tās izstrādes un paredzētajam mērķim. Piemēram, Mikroshēmas ierīču izmantošana un Mikroshēmas karšu apstrāde ar magnētisko joslu vai manuālu ievadi NAV efektīvs šīs tehnoloģijas izmantošanas veids.
- Tirdzniecības vietu procentuālais īpatsvars, kas izmanto Risku mazināšanas tehnoloģiju, tiek noteikts PFI izmeklēšanā.
- Zaudējumu atlīdzināšanas pienākuma apmēra samazinājums neattiecas uz jebkuru neatbilstības maksu, kas maksājama saistībā ar Datu incidentu.

Piem.	Izmantotās Riska mazināšanas tehnoloģijas	Vai tiesības saņemt paaugstinātu Zaudējumu atlīdzības saistību samazinājumu?	Samazinājums
1	80% darījumu ar Mikroshēmas ierīcēm	Nē	50%: Standarta samazinājums (mazāk kā 75% Riska mazināšanas tehnoloģiju lietojums nekvalificējas Paaugstinātam samazinājumam)[1]
	0% atrašanās vietu izmantota cita Riska mazināšanas tehnoloģija		
2	80% Darījumu ar Mikroshēmu ierīcēm	Jā	77%: Paaugstināts samazinājums (pamatojoties uz 77% Riska mazināšanas tehnoloģijas izmantošanu)
	77% atrašanās vietu izmantota cita Riska mazināšanas tehnoloģija		

Piem.	Izmantotās Riska mazināšanas tehnoloģijas	Vai tiesības saņemt paaugstinātu Zaudējumu atlīdzības saistību samazinājumu?	Samazinājums
3	93% darījumu ar Mikroshēmas ierīcēm 100% atrašanās vietu izmantota cita Riska mazināšanas tehnoloģija	Jā	93%: Paaugstināts samazinājums (pamatojoties uz 93% Darījumu ar Mikroshēmas ierīcēm)
4	40% darījumu ar Mikroshēmas ierīcēm 90% atrašanās vietu izmantota cita Riska mazināšanas tehnoloģija	Nē	50%: Standarta samazinājums (mazāk nekā 75% Darījumu ar Mikroshēmas ierīcēm nekvalificējas Paaugstinātam samazinājumam)

[1] Datu Incidents, kurā iesaistīti 10 000 American Express Karšu kontu, piemērojot 5 USD par katru konta numuru (10 000 x 5 USD = 50 000 USD), var kvalificēties 50% samazinājumam (zaudējumu atlīdzināšanas pienākuma apmērs tiek samazināts no 50 000 USD līdz 25 000 USD), atskaitot jebkādu neatbilstības maksu.

Sadaļa 4 Svarīga periodiska jūsu sistēmu validācija

Jums ir jāveic turpmāk minētās darbības, lai saskaņā ar PCI DSS katru gadu un reizi ceturksnī pārbaudītu, kā aprakstīts zemāk, to jūsu un jūsu Franšīzes ņēmēju iekārtu, sistēmu un/vai tīklu (un to komponentu) statusu, kuros tiek uzglabāti, apstrādāti vai pārraidīti Kartes lietotāja dati vai Sensitīvie autentifikācijas dati.

Lai veiktu validāciju, ir nepieciešams veikt četras darbības:

Darbība 1: dalība American Express Atbilstības programmā atbilstoši šai politikai.

Darbība 2: sava līmeņa un validācijas prasību izprašana.

Darbība 3: American Express sūtāmās validācijas dokumentācijas aizpildīšana.

Darbība 4: validācijas dokumentācijas nosūtīšana American Express noteiktajā laikā.

Darbība 1: Dalība American Express Atbilstības programmā atbilstoši šai politikai

1. līmeņa Tirgotājiem, 2. līmeņa Tirgotājiem un visiem pakalpojumu sniedzējiem, ir jāpiedalās American Express' PCI Atbilstības programmā atbilstoši šai politikai, norādot pilnu vārdu, e-pasta adresi, tālruņa numuru un tās personas pasta adresi, kura rīkojas kā par datu drošību atbildīgā persona. Jums jāiesniedz šī informācija SecureTrust, kas ir Trustwave nodaļa (https://portal.securetrust.com), kas administrē programmu American Express vārdā, izmantojot kādu no metodēm, kas minēta Darbība 4: „Validācijas dokumentu nosūtīšana American Express". Jums jāpaziņo SecureTrust, ja šī informācija ir mainījusies, sniedzot atjaunināt informāciju, ja tāda ir. Ja šāda informācija netiks iesniegta, tas neietekmēs jūsu tiesības aprēķināt maksu par validācijas neveikšanu, kas norādītas Validācijas neesamības maksu tabula.

American Express pēc saviem ieskatiem var pieprasīt noteiktiem 3. līmeņa un 4. līmeņa Tirgotājiem piedalīties American Express atbilstības programmā atbilstoši šai politikai, nosūtot viniem rakstisku paziņojumu. Tirgotājam ir jāreģistrējas ne vēlāk kā 90 dienu laikā pēc paziņojuma saņemšanas.

Darbība 2: Sava līmeņa un validācijas prasību izprašana

Tirgotājiem ir noteikti četri līmeņi, un Pakalpojumu Sniedzējiem - divi līmeņi, pamatojoties uz jūsu American Express Karšu Darījumu apjomu. Tirgotājiem tas ir to Iestāžu iesniegtais apjoms, kas atbilst augstākajam American Express Tirgotāja konta līmenim.* Jūs tiksiet klasificēts vienā no līmeņiem, kas norādīti Tirgotāju un Pakalpojumu sniedzēju tabulās zemāk. Uzņēmumu ierosināto maksājumu (BIP) darījumi netiek iekļauti American Express Karšu darījumu apjomā Tirgotāja līmeņa un validācijas prasību noteikšanas nolūkā.

* Franšīzes Devēju gadījumā tas ietver apjomu no viņu Franšīzes ņēmēju Iestādēm. Franšīzes devējiem, kuri pieprasa, lai viņu Franšīzes ņēmēji izmantotu konkrētu Pārdošanas Punkta (POS) Sistēmu vai Pakalpojumu Sniedzēju, jāiesniedz arī validācijas dokumentācija par attiecīgajiem Franšīzes ņēmējiem.

Tirgotājiem izvirzītās prasības

Tirgotājiem (nevis Pakalpojumu Sniedzējiem) noteiktas četras iespējamās klasifikācijas attiecībā uz viņu līmeni un validācijas prasībām. Pēc Tirgotāja līmeņa noteikšanas atbilstoši zemāk esošajam sarakstam skatiet Tirgotāju tabulu, lai noteiktu Audita Dokumentācijas prasības.

- **1. līmeņa Tirgotājs** – 2,5 miljoni vai vairāk American Express Karšu darījumu gadā, vai jebkurš Tirgotājs, kuru American Express citādi pieskaita 1. līmenim.
- **2. līmeņa Tirgotājs** – 50 000 līdz 2,5 miljoni American Express Karšu darījumu gadā.
- **3. līmeņa Tirgotājs** – 10 000 līdz 50 000 American Express Karšu darījumu gadā.
- **4. līmeņa Tirgotājs** – mazāk nekā 10 000 American Express Karšu darījumu gadā.

Tirgotāju tabula

	Validācijas dokumentācija		
Tirgotāja līmenis/ American Express Darījumi gadā	Klātienes novērtējuma ziņojums par atbilstību (ROC)	Pašnovērtējuma anketa (SAQ) UN ikceturkšņa tīkla skenēšana	STEP atestācija Tirgotājiem, kas kvalificējas
1. līmenis/ 2,5 miljoni vai vairāk	Obligāti	Nav attiecināms	Izvēles (aizstāj ROC)
2. līmenis/ 50 000 līdz 2,5 miljoni	Izvēles	SAQ obligāts (ja netiek iesniegts Klātienes vērtējums); skenēšana obligāta ar noteiktiem SAQ veidiem	Izvēles (aizstāj SAQ un tīkla skenēšanu vai ROC)
3. līmenis/ 10 000 līdz 50 000	Izvēles	SAQ izvēles (obligāts, ja to pieprasa American Express); skenēšana obligāta ar noteiktiem SAQ veidiem	Izvēles (aizstāj SAQ un tīkla skenēšanu vai ROC)
4. līmenis/ 10 000 vai mazāk	Izvēles	SAQ izvēles (obligāts, ja to pieprasa American Express); skenēšana obligāta ar noteiktiem SAQ veidiem	Izvēles (aizstāj SAQ un tīkla skenēšanu vai ROC)

* Pārpratumu novēršanai ņemiet vērā, ka 3. līmeņa un 4. līmeņa Tirgotājiem nav jāiesniedz Validācijas dokumentācija, ja vien American Express to nenosaka pēc saviem ieskatiem, taču šiem Tirgotājiem ir jāatbilst, un tie ir atbildīgi par visu šīs Datu drošības darbības politikas noteikumu ievērošanu.

American Express patur tiesības pārbaudīt PCI validācijas dokumentācijas precizitāti un atbilstību atbilstoši nepieciešamībai, tostarp pēc mūsu izvēles iesaistot QSA vai PFI uz American Express rēķina.

Drošības tehnoloģiju uzlabošanas programma (STEP)

Tirgotāji, kas atbilst PCI DSS, pēc American Express ieskatiem var kvalificēties arī Drošības tehnoloģijas uzlabošanas programmai (STEP), ja viņi savās Karšu apstrādes vidēs ievieš noteiktas papildu drošības tehnoloģijas. STEP ieviešama tikai tādā gadījumā, ja Tirgotājs iepriekšējos 12 mēnešos nav saskāries ar Datu incidentu, un 75% no visiem Tirgotāja Karšu Darījumiem tiek veikti, izmantojot:

- **EMV** – aktīvā mikroshēmā iespējotā ierīcē, kurai ir derīgs un spēkā esošs EMVCo (www.emvco.com) apstiprinājums/sertifikācija un kas spēj apstrādāt AEIPS prasībām atbilstošus Mikroshēmas karšu darījumus. (ASV Tirgotājiem jāiekļauj bezkontakta)
- **Divpunktu šifrēšanu (P2PE)** – kas paziņota Tirgotāja Starpniekiestādei, izmantojot PCI SSC apstiprinātu vai QSA apstiprinātu Divpunktu šifrēšanas sistēmu

Tirgotājiem, kuri ir tiesīgi saņemt Drošības Tehnoloģiju Uzlabošanas Programmu, ir samazinātas PCI Audita Dokumentācijas prasības, kā aprakstīts zemāk Darbība 3: „American Express nosūtāmo validācijas dokumentu aizpildīšana“.

Pakalpojumu sniedzējiem izvirzītās prasības

Pakalpojumu sniedzējiem (nevis Tirgotājiem) noteiktas divas iespējamās klasifikācijas attiecībā uz viņu līmeni un validācijas prasībām. Pēc Pakalpojumu sniedzēja līmeņa noteikšanas atbilstoši zemāk esošajam sarakstam skatiet Pakalpojumu Sniedzēju tabulu, lai noteiktu validācijas dokumentācijas prasības.

1. līmeņa Pakalpojumu sniedzējs – 2,5 miljoni vai vairāk American Express Karšu darījumu gadā; vai jebkurš Pakalpojumu sniedzējs, kuru American Express citādi uzskata par 1. līmeņa Pakalpojumu sniedzēju.

2. līmeņa Pakalpojumu sniedzējs – mazāk nekā 2,5 miljoni American Express Karšu darījumu gadā; vai jebkurš Pakalpojumu sniedzējs, kuru American Express citādi neuzskata par 1. līmeņa Pakalpojumu sniedzēju.

Pakalpojumu Sniedzēji nav tiesīgi saņemt STEP.

Pakalpojumu sniedzēju tabula

Līmenis	Validācijas dokumentācija	Prasība
1	Klātienes drošības novērtējuma ziņojums par atbilstību	Obligāti
2	Ikgadējā SAQ D (Pakalpojumu sniedzējs) un Ikceturkšņa tīkla skenēšana vai Ikgadējais klātienes drošības novērtējuma ziņojums par atbilstību, ja izvēlas to.	Obligāti

Ieteicams, ka Pakalpojumu Sniedzēji nodrošina atbilstību PCI noteikto papildu validāciju noteiktiem uzņēmumiem.

Darbība 3: American Express nosūtāmo validācijas dokumentu aizpildīšana

Turpmāk minētie dokumenti ir nepieciešami dažādiem Tirgotāju un Pakalpojumu sniedzēju līmeņiem, kas uzskaitīti augstāk Tirgotāju tabulā un Pakalpojumu Sniedzēju tabulā.

Ikgadējais klātienes drošības novērtējums – Ikgadējais klātienes drošības novērtējums ir detalizēta jūsu iekārtu, sistēmu un tīklu (un to komponentu), kuros tiek uzglabāti, apstrādāti vai pārraidīti Kartes lietotāja Dati vai Sensitīvie autentifikācijas dati (vai abi), pārbaude uz vietas. Novērtējums jāveic:

- QSA, vai
- jums un jāapstiprina jūsu izpilddirektoram, finanšu direktoram, galvenajam informācijas drošības speciālistam vai vadītājam un katru gadu jāiesniedz American Express par piemērojamu Atbilstības apliecinājumu (AOC).

AOC ir jāapliecina atbilstība visām PCI DSS prasībām, un pēc pieprasījuma tajā jāiekļauj pilnīga ziņojuma atbilstību kopijas (1. līmeņa Tirgotājiem un 1. līmeņa Pakalpojumu sniedzējiem).

Ikgadējā pašnovērtējuma anketa – Ikgadējais pašnovērtējums ir process, kurā tiek izmantota PCI DSS SAQ, kas ļauj veikt pašpārbaudi jūsu iekārtām, sistēmām un tīkliem (un to komponentēm), kur tiek uzglabāti, apstrādāti vai pārsūtīti Kartes lietotāja dati vai Sensitīvie autentifikācijas dati (vai abi). Pašnovērtējums ir jāveic jums, un tas ir jāapstiprina jūsu izpilddirektoram, finanšu direktoram, galvenajam informācijas drošības speciālistam vai vadītājam. SAQ AOC sadaļa ir jāiesniedz American Express katru gadu. SAQ AOC sadaļā ir jāapliecina atbilstība visām PCI DSS prasībām, un pēc pieprasījuma tajā jāiekļauj pilnīgas SAQ kopijas (2. līmeņa, 3. līmeņa un 4. līmeņa Tirgotājiem; 2. Līmeņa Pakalpojumu sniedzējiem).

Tīkla ikceturkšņa skenēšana – Tīkla ikceturkšņa skenēšana ir process, kas attālināti pārbauda jūsu internetam pieslēgtos datortīklus un tīmekļa serverus, lai konstatētu to iespējamos trūkumus un ievainojamību. Tas jāveic Apstiprinātam skenēšanas pakalpojumu sniedzējam (**ASV**). Jums reizi ceturksnī ir jāveic un jāiesniedz American Express ASV Skenēšanas atbilstības apliecinājums (**AOSC**) skenēšanas rezultātu kopsavilkums (un pēc pieprasījuma pilnīgas skenēšanas kopijas). AOSC vai kopsavilkumam jāapstiprina, ka rezultāti atbilst PCI DSS pārbaudes procedūrām, ka netika identificētas augsta riska problēmas un ka pārbaude ir pabeigta vai atbilstoša (visi Tirgotāji, izņemot tos, kuri arī iesniedz Darba vietas drošības novērtējuma ziņojumu, STEP piemērotos Tirgotājus un visus Pakalpojumu sniedzējus). Lai izvairītos no šaubām, Ceturkšņa tīkla pārbaudes ir obligātas, ja to pieprasa atbilstošā SAQ.

Ikgadējā STEP atestācijas validācijas dokumentācija – American Express Ikgadējā STEP kvalifikācijas atestācija („STEP Atestācija") ir pieejama tikai tiem Tirgotājiem, kuri atbilst Darbība 2: „Sava līmeņa un validācijas prasību izprašana". STEP Atestācija ietver procesu, kurā tiek izmantotas PCI DSS prasības, kas ļauj veikt pašpārbaudi jūsu iekārtām, sistēmām un tīkliem (un to komponentiem), kur tiek uzglabāti, apstrādāti vai pārsūtīti Kartes lietotāja dati vai Sensitīvie autentifikācijas Dati (vai abi). Pašnovērtējums ir jāveic jums, un tas ir jāapstiprina jūsu izpilddirektoram, finanšu direktoram, galvenajam informācijas drošības speciālistam vai vadītājam. Jums ir jāveic process, katru gadu iesniedzot American Express STEP Atestācijas veidlapu. (Vienīgi Tirgotājiem, kuriem ir tiesības izmantot STEP). Ikgadējā STEP Atestācijas veidlapa ir pieejama lejupielādei no SecureTrust drošā portāla.

Atbilstības pārskats – Atbilstības pārskats (SOC) ir dokuments, ar kuru Franšīzes devējs vai Pakalpojumu sniedzējs var ziņot par savu Franšīzes ņēmēju PCI atbilstības statusu. SOC veidne ir pieejama lejupielādei, izmantojot SecureTrust drošo portālu.

Neatbilstība PCI DSS – Ja jūs nenodrošināt atbilstību PCI DSS, jums jāiesniedz viens no šādiem dokumentiem:

- Atbilstības apstiprināšana (AOC), tostarp "4. daļa. Rīcības plāns neatbilstības gadījumā"
- PCI Prioritārās pieejas rīka kopsavilkums un Atbilstības apstiprināšana (PASAOC)
- Projekta plāna veidne (pieejama lejupielādei no SecureTrust drošā portāla)

Katrā no iepriekš minētajiem dokumentiem ir jānosaka novēršanas termiņš, kas nepārsniedz 12 mēnešus pēc dokumenta pabeigšanas datuma, lai sasniegtu atbilstību. Jums jāiesniedz atbilstošais dokuments American Express, izmantojot kādu no metodēm, kas minētas Darbība 4: „Validācijas dokumentu nosūtīšana American Express". Jums regulāri jāinformē American Express par sava Neatbilstības statusa problēmas novēršanas progresu (1. līmeņa, 2. līmeņa, 3. līmeņa un 4. līmeņa Tirgotāji, visi Pakalpojumu sniedzēji). Lai izvairītos no pārpratumiem, Tirgotāji, kas neatbilst PCI DSS, nekvalificējas STEP. American Express neiekasēs no jums (zemāk aprakstītās) validācijas neesamības maksas par neatbilstību pirms neatbilstības novēršanas datuma, tomēr jūs joprojām esat atbildīgi pret American Express par visām zaudējumu atlīdzības saistībām Datu incidenta gadījumā, un jums ir jāievēro visi pārējie šīs politikas noteikumi.

Darbība 4: Validācijas dokumentu nosūtīšana American Express

Visiem Tirgotājiem un Pakalpojumu sniedzējiem, kam ir jāpiedalās American Express PCI Atbilstības programmā, ir jāiesniedz Validācijas dokumentācija, kas atzīmētas kā "obligāti" tabulās Darbība 2: „Sava līmeņa un validācijas prasību izprašana“. Jums ir jāiesniedz Validācijas dokumentācija SecureTrust, izmantojot vienu no šīm metodēm:

- **Drošs portāls**: Validācijas dokumentāciju var augšupielādēt SecureTrust drošā portālā https://portal.securetrust.com.

  Lūdzu, sazinieties ar SecureTrust pa tālruni, kas norādīts jūsu Valstij, vai e-pastu americanexpresscompliance@securetrust.com, lai saņemtu norādījumus par šī portāla izmantošanu.
- **Drošs fakss**: Validācijas dokumentāciju var nosūtīt pa faksu: +1 (312) 276-4019. (+ norāda starptautiskā tiešā numura „IDD" prefiksu, piemēro starptautiskā zvana tarifu).

  Lūdzu, norādiet jūsu nosaukumu, DBA (Doing Business As) nosaukumu, jūsu datu drošības kontaktpersonas vārdu un uzvārdu, jūsu adresi, tālruņa numuru un, tikai Tirgotājiem, jūsu 10 ciparu American Express Tirgotāja Numuru.

Ja jums rodas vispārīgi jautājumi par augstāk minētoprogrammu vai procesu, lūdzu, sazinieties ar SecureTrust pa tālruņa numuru + 800 9000 1140 vai +1 (312) 267-3208, vai e-pastu americanexpresscompliance@securetrust.com.

Atbilstības nodrošināšanas un validācijas izdevumus sedzat jūs. Iesniedzot Validācijas dokumentāciju, jūs apliecināt un garantējat American Express, ka jums ir tiesības atklāt tajā ietverto informāciju, un iesniedzat American Express Validācijas dokumentāciju, nepārkāpjot nevienas citas personas tiesības.

Tirgi	SecureTrust tālruņa numurs
Apvienotā Karaliste	+ 800 9000 1140
Argentīna	+ 800 9000 1140
Austrālija	+ 800 9000 1140
Austrija	+ 800 9000 1140
Bulgārija	+ 312 267 3208
Čehijas Republika	+ 800 144 316
Dānija	+ 800 9000 1140
Francija	+ 800 9000 1140
Grieķija	+ 312 267 3208
Honkonga	+ 800 9000 1140
Horvātija	+ 312 267 3208
IDC	+ 888 900 0114
Igaunija	+ 312 267 3208
Indija	+ 800 9000 1140
Īrija	+ 800 9000 1140
Islande	+ 800 9000 1140
Itālija	+ 800 9000 1140
Japāna	+ 312 267 3208
Jaunzēlande	+ 800 9000 1140
Kanāda	1 866 659 9016

Tirgi	SecureTrust tālruņa numurs
Kipra	+ 800 9000 1140
Krievija	+ 312 267 3208
Latvija	+ 312 267 3208
Lietuva	+ 312 267 3208
Malta	+ 312 267 3208
Meksika	+ 888 900 0114
Nīderlande	+ 312 267 3208
Norvēģija	+ 800 9000 1140
Polija	+ 800 9000 1140
Portugāle	+ 312 267 3208
Rumānija	+ 312 267 3208
Savienotās Valstis	1 866 659 9016
Singapūra	+ 800 9000 1140
Slovākija	+ 312 267 3208
Slovēnija	+ 312 267 3208
Spānija	+ 800 9000 1140
Taivāna	+ 312 267 3208
Taizeme	+ 800 9000 1140
Ungārija	+ 800 9000 1140
Vācija	+ 800 9000 1140
Zviedrija	+ 800 9000 1140

+ norāda starptautiskā tiešā numura „IDD" prefiksu, piemēro starptautiskā zvana tarifu.

Validācijas neveikšanas maksas un Līguma izbeigšana

American Express ir tiesīga iekasēt no jums validācijas neesamības maksas un izbeigt Līgumu, ja jūs neizpildāt šīs prasības vai neiesniedzat obligāto Validācijas dokumentāciju American Express līdz noteiktajam termiņam. American Express paziņos jums atsevišķi katram gada un ceturkšņa pārskata periodam noteikto termiņu.

Nosūtiet dokumentāciju American Express līdz attiecīgajam termiņam. American Express paziņos jums atsevišķi katram gada un ceturkšņa pārskata periodam noteikto termiņu. Maksas, kas attiecināmas uz jūsu Valsti, skatīt Validācijas neesamības maksu tabulā turpmāk dokumentā.

Apraksts	1. līmeņa Tirgotājs vai 1. līmeņa Pakalpojumu sniedzējs	2. līmeņa Tirgotājs, 2. līmeņa Pakalpojumu sniedzējs vai STEP Tirgotājs	3. līmeņa vai 4. līmeņa Tirgotājs
Maksu par validācijas neveikšanu aprēķinās, ja Validācijas dokumentācija nav saņemta līdz pirmajam termiņam.	1. mēneša maksa par 1. līmeni	1. mēneša maksa par 2. līmeni	Mēneša maksa
Papildu maksu par validācijas neveikšanu aprēķinās, ja Validācijas dokumentācija nav saņemta 30 dienu laikā pēc pirmā termiņa.	2. mēneša maksa par 1. līmeni	2. mēneša maksa par 2. līmeni	
Papildu maksu par validācijas neveikšanu aprēķinās, ja Validācijas dokumentācija nav saņemta 60 dienu laikā pēc pirmā termiņa.	3. mēneša maksa par 1. līmeni	3. mēneša maksa par 3. līmeni	

Ja American Express nesaņems no jums obligāti iesniedzamo Validācijas dokumentāciju 60 dienu laikā pēc pirmā termiņa, American Express ir tiesīgs izbeigt Līgumu atbilstoši tā noteikumiem un kumulatīvi piemērot jums kopējo validācijas neesamības maksu.

Validācijas neesamības maksu tabula

Tirgus	Līmenis	Tips	Valūta	1. mēneša maksa	2. mēneša maksa	3. mēneša maksa
Apvienotā Karaliste	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	GBP	12 500	18 000	23 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	GBP	2 500	5 000	7 500
	3. līmenis un 4. līmenis	Tirgotājs	GBP	Mēneša maksa: 15		
Austrālija	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	AUD	35 000	49 000	63 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	AUD	7 000	14 000	21 000
	3. līmenis un 4. līmenis	Tirgotājs	AUD	Mēneša maksa: 20		

Tirgus	Līmenis	Tips	Valūta	1. mēneša maksa	2. mēneša maksa	3. mēneša maksa
Bulgārija	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	BGN	28 000	40 000	51 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	BGN	5 500	11 000	16 500
	3. līmenis un 4. līmenis	Tirgotājs	BGN	Mēneša maksa: 33		
Čehijas Republika	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	CZK	392 000	564 000	721 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	CZK	78 300	157 000	235 000
	3. līmenis un 4. līmenis	Tirgotājs	CZK	Mēneša maksa: 440		
Dānija	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	DKK	110 000	156 000	200 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	DKK	22 000	42 000	65 000
	3. līmenis un 4. līmenis	Tirgotājs	DKK	Mēneša maksa: 130		
Honkonga	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	HKD	25 000	35 000	45 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	HKD	5 000	10 000	15 000
	3. līmenis un 4. līmenis	Tirgotājs	HKD	Mēneša maksa: 150		
Horvātija	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	HRK	105 000	152 000	195 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	HRK	21 000	42 000	63 000
	3. līmenis un 4. līmenis	Tirgotājs	HRK	Mēneša maksa: 130		

Tirgus	Līmenis	Tips	Valūta	1. mēneša maksa	2. mēneša maksa	3. mēneša maksa
Islande	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	ISK	3 070 000	4 300 000	5 500 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	ISK	615 000	920 000	1 227 200
	3. līmenis un 4. līmenis	Tirgotājs	ISK	Mēneša maksa: 2 400		
Jaunzēlande	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	NZD	35 000	49 000	63 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	NZD	7 000	14 000	21 000
	3. līmenis un 4. līmenis	Tirgotājs	NZD	Mēneša maksa: 20		
Kipra, Igaunija, Francija, Vācija, Īrija, Spānija, Latvija, Lietuva, Portugāle, Slovākija, Slovēnija	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	EUR	19 000	26 000	34 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	EUR	4 000	7 500	11 000
	3. līmenis un 4. līmenis	Tirgotājs	EUR	Mēneša maksa: 15		
Norvēģija	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	NOK	135 000	195 000	249 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	NOK	27 000	54 000	81 000
	3. līmenis un 4. līmenis	Tirgotājs	NOK	Mēneša maksa: 170		
Singapūra	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	SGD	38 000	53 000	68 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	SGD	7 500	15 000	22 500
	3. līmenis un 4. līmenis	Tirgotājs	SGD	Mēneša maksa: 25		

Tirgus	Līmenis	Tips	Valūta	1. mēneša maksa	2. mēneša maksa	3. mēneša maksa
Ungārija	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	HUF	4 650 000	6 700 000	8 600 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	HUF	930 000	1 860 000	2 800 000
	3. līmenis un 4. līmenis	Tirgotājs	HUF	Mēneša maksa: 5 500		
Zviedrija	1. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	SEK	175 000	245 000	315 000
	2. līmenis	Tirgotājs vai Pakalpojuma sniedzējs	SEK	35 000	70 000	105 000
	3. līmenis un 4. līmenis	Tirgotājs	SEK	Mēneša maksa: 135		

Sadaļa 5 Konfidencialitāte

American Express veiks saprātīgus pasākumus, lai ievērotu (un liktu tās aģentiem un apakšuzņēmējiem, tostarp SecureTrust, ievērot) jūsu ziņojumu par atbilstību, tostarp Validācijas dokumentācijas konfidencialitāti un neatklāt Validācijas dokumentāciju nevienai trešai personai (izņemot American Express saistītās personas, aģentus, pārstāvjus, Pakalpojumu sniedzējus un apakšuzņēmējus) trīs gadus no saņemšanas dienas, izņemot to, ka šis konfidencialitātes pienākums neattiecas uz Validācijas dokumentāciju, kas:

a. jau ir zināma American Express pirms izpaušanas;

b. ir vai kļūst publiski pieejama, American Express nepārkāpjot šo punktu;

c. ir American Express tiesiski saņemta no trešās personas bez konfidencialitātes ievērošanas pienākuma;

d. ir American Express neatkarīgi izstrādāta; vai

e. ir prasīta izpaust ar tiesas, administratīvās iestādes vai valsts iestādes rīkojumu vai ar jebkuru likumu, normatīvo aktu vai regulu, vai ar tiesas pavēsti, pieprasījumu, uzaicinājumu vai citu administratīvo vai tiesisko procesu, vai ar jebkādu oficiālu vai neoficiālu izmeklēšanu, kuru veic kāda valsts aģentūra vai iestāde (tajā skaitā jebkurš regulators, inspektors, revidents vai tiesībaizsardzības aģentūra).

Sadaļa 6 Saistību atruna

AMERICAN EXPRESS AR ŠO ATSAKĀS NO JEBKURIEM UN VISIEM SKAIDRI IZTEIKTIEM, IZRIETOŠIEM, LIKUMĀ PAREDZĒTIEM VAI CITA VEIDA APLIECINĀJUMIEM, GARANTIJĀM UN SAISTĪBĀM ATTIECĪBĀ UZ ŠO DATU DROŠĪBAS DARBĪBAS POLITIKU, PCI DSS, EMV SPECIFIKĀCIJĀM, KĀ ARĪ QSA, ASV VAI PFI (VAI JEBKURU NO VIŅIEM) IECELŠANU VAI DARBĪBU, TAJĀ SKAITĀ JEBKĀDU GARANTIJU PAR PIEMĒROTĪBU PĀRDOŠANAI VAI LIETOŠANAI KONKRĒTAM MĒRĶIM. AMERICAN EXPRESS KARŠU IZDEVĒJI NAV TREŠO PERSONU PATIESĀ LABUMA GUVĒJI SASKAŅĀ AR ŠO POLITIKU.

Noderīgas tīmekļa vietnes

American Express Datu drošība: www.americanexpress.com/datasecurity

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

Terminu saraksts

Tikai šīs Datu drošības darbības politika (DSOP) mērķiem tiek lietotas šādas definīcijas, kas ir noteicošas, ja rodas pretrunas starp terminiem, kas iekļauti *tirgotāju noteikumi*.

1. līmeņa Tirgotājs ir Tirgotājs ar 2,5 miljonu vai vairāk American Express Karšu darījumiem gada laikā vai jebkurš Tirgotājs, kuru American Express citādi pieskaita 1. līmenim.

2. līmeņa Tirgotājs ir Tirgotājs ar 50 000 līdz 2,5 miljoniem American Express Karšu darījumu gadā.

3. līmeņa Tirgotājs ir Tirgotājs ar 10 000 līdz 50 000 American Express Karšu darījumu gadā.

4. līmeņa Tirgotājs ir Tirgotājs ar mazāk nekā 10 000 American Express Karšu darījumu gadā.

1. līmeņa Pakalpojumu sniedzējs ir Pakalpojumu sniedzējs ar 2,5 miljonu vai vairāk American Express Karšu darījumu gadā; vai jebkurš Pakalpojumu sniedzējs, kuru American Express citādi uzskata par 1. līmeņa Pakalpojumu sniedzēju.

2. līmeņa Pakalpojumu sniedzējs ir Pakalpojumu sniedzējs ar mazāk nekā 2,5 miljoni American Express Karšu darījumu gadā; vai jebkurš Pakalpojumu sniedzējs, kuru American Express citādi neuzskata par 1. līmeņa Pakalpojumu sniedzēju.

American Express karte vai **Karte** ir jebkura karte, konta piekļuves ierīce, maksājumu ierīce vai pakalpojums, kurā norādīts American Express vai saistītās personas nosaukums, logotips, preču zīme, pakalpojumu zīme, tirdzniecības nosaukums, cits patentēts dizains vai apzīmējums un kuru izdevis izdevējs, vai kartes konta numurs.

Apdraudētās Kartes Numurs ir American Express Kartes konta numurs, kas saistīts ar Datu incidentu.

Apstiprinātais divpunktu šifrēšanas (P2PE) risinājums, kas iekļauts PCI SSC validēto risinājumu sarakstā vai kuru apstiprinājusi Maksājumu karšu nozares Drošības Standartu Padomes (PCI SSC) Kvalificēts drošības novērtētājs (P2PE Uzņēmums).

Apstiprināts skenēšanas pakalpojumu sniedzējs (ASV) ir uzņēmums, kuram ir piešķirta Payment Card Industry Security Standards Council, LLC licence, lai apstiprinātu noteiktu PCI DSS prasību ievērošanu, veicot interneta vides ievainojamības skenēšanu.

Aptvertās personas ir jebkuri jūsu darbinieki, aģenti, pārstāvji, apakšuzņēmēji, Apstrādātāji, jūsu tirdzniecības punkta aprīkojuma vai sistēmu, vai maksājumu apstrādes risinājumu Pakalpojumu sniedzēji, uzņēmumi, kas saistīti ar jūsu American Express Tirgotāja kontu, un jebkura cita persona, kurai jūs saskaņā ar Līgumu varat sniegt piekļuvi Kartes turētāja datiem vai Sensitīviem autentifikācijas datiem (vai abiem).

Atbilstības apliecinājums (AOC) ir paziņojums par jūsu atbilstību Maksājumu karšu nozares Datu Drošības Standartam (PCI DSS) atbilstoši Payment Card Industry Security Standards Council, LLC noteiktajam veidam.

Atbilstības pārskats (SOC) ir PCI validācijas dokuments, kuru Franšīzes devējs vai Pakalpojumu sniedzējs izmanto, lai norādītu savu Franšīzes ņēmēju PCI atbilstības statusu.

Darījums ir Maksājums vai Kredīts, kas veikts, izmantojot Karti.

Datu incidents ir incidents, kas ietver American Express Šifrēšanas atslēgu apdraudēšanu, vai vismaz viens American Express Kartes konta numurs, kurā notiek:

- nesankcionēta piekļuve Šifrēšanas atslēgām, Kartes lietotāja datiem vai Sensitīviem autentifikācijas datiem (vai to kombinācijai), kas tiek glabāti, apstrādāti vai pārraidīti jūsu vai jūsu lietošanai sankcionētajās iekārtās, sistēmās un/vai tīklos (vai to komponentos), kā arī to nesankcionēta izmantošana;
- šādu Šifrēšanas Atslēgu, Kartes Lietotāja Datu vai Sensitīvo autentifikācijas datu (vai to kombinācijas) izmantošana, kas nenotiek saskaņā ar Līgumu; un/vai
- jebkādu datu nesēju, materiālu, ierakstu vai informācijas, kas satur šādas Šifrēšanas atslēgas, Kartes lietotāja datus vai Sensitīvos autentifikācijas datus (vai to kombināciju), iespējams vai apstiprināts zudums, zādzība vai nelikumīga piesavināšanās.

Datu incidentu gadījuma logs ir periods, kas sākas apdraudējuma datumā, ja tas zināms, vai 365 dienas pirms Paziņojuma Datuma ja faktiskais apdraudējuma datums nav zināms. Datu incidentu gadījumu logs beidzas 30 dienas pēc Paziņojuma datuma.

Divpunktu šifrēšana (P2PE) ir risinājums, kas kriptogrāfiski aizsargā konta datus no punkta, kur Tirgotājs pieņem norēķinu karti, līdz drošam atšifrēšanas punktam.

Drošības tehnoloģiju uzlabošanas programma (STEP) ir American Express programma, kurā Tirgotāji tiek mudināti izmantot tehnoloģijas, kuras uzlabo datu drošību. Lai kvalificētos STEP, Tirgotājiem nedrīkst būt Datu Incidentu 12 mēnešus pirms STEP Atestācijas iesniegšanas un vismaz 75% no visiem Darījumiem ir jābūt veiktiem, izmantojot Divpunktu šifrēšanu vai Mikroshēmu ierīces klātienē.

EMV darījums ir integrētās shēmas kartes (dažreiz saukta arī „IC Karte", „mikroshēmas karte", viedkarte", „EMV karte" vai „ICC") darījums, kuru veic ar IC karti, ko pieņem pārdošanas punkta (POS) terminālis ar derīgu un pašreizēju EMV tipa apstiprinājumu. EMV tipa apstiprinājumi ir pieejami vietnē www.emvco.com.

EMV specifikācijas ir EMVCo, LLC izdotas specifikācijas, kas ir pieejamas vietnē www.emvco.com.

Franšīzes devējs ir uzņēmuma īpašnieks, kurš licencē personas vai organizācijas (Franšīzes ņēmējus) izplatīt preces un/vai pakalpojumus ar īpašnieka Zīmi vai darboties, izmantojot īpašnieka Zīmi; sniedz palīdzību Franšīzes ņēmējiem viņu komercdarbības veikšanā vai ietekmē Franšīzes ņēmēja darbības veidu, kā arī pieprasa Franšīzes Ņēmējiem maksas samaksu.

Kartes lietotāja dati ir lietoti ar nozīmi, kas šim terminam noteikta PCI DSS terminu sarakstā.

Kartes lietotāja informācija ir informācija par American Express Kartes lietotājiem un Karšu darījumiem, ieskaitot vārdus un uzvārdus, adreses, kartes konta numurus un kartes identifikācijas numurus (CID).

Kartes lietotājs ir fiziska vai juridiska persona, (i) kura ir noslēgusi ar izdevēju līgumu par Kartes konta izveidošanu, vai (ii) kuras vārds un uzvārds parādās uz Kartes.

Kredīts ir Maksājuma summa, kuru jūs atmaksājat Kartes lietotājiem par pirkumiem vai maksājumiem, kas veikti, izmantojot Karti.

Kvalificēts drošības novērtētājs (QSA) ir Payment Card Industry Security Standards Council, LLC apstiprināta organizācija, kura apstiprina PCI DSS ievērošanu.

Maksājuma pieteikums ir lietots ar nozīmi, kāda tam noteikta spēkā esošajā Maksājumu karšu nozares maksājumu pieteikumu datu drošības standartu terminu sarakstā, kas ir pieejams tīmekļa vietnē www.pcisecuritystandards.org.

Maksājums ir maksājums vai pirkums, kas veikts, izmantojot Karti.

Maksājumu karšu nozares drošības standartu padomes (PCI SSC) prasības ir standartu un prasību kopums, ks saistīts ar maksājumu karšu datu nodrošināšanu un aizsardzību, tostarp PCI DSS un PA DSS, kas pieejams tīmekļa vietnē www.pcisecuritystandards.org.

Mikroshēma ir integrēta Kartē iegulta mikroshēma, kas satur Kartes lietotāja un konta informāciju.

Mikroshēmas ierīce ir pārdošanas punkta ierīce, kurai ir derīgs un spēkā esošs EMVCo (www.emvco.com) apstiprinājums/sertifikācija un kas spēj apstrādāt AEIPS prasībām atbilstošus Mikroshēmas karšu darījumus.

Mikroshēmas karte ir Karte, kas satur mikroshēmu un var pieprasīt PIN, lai pārbaudītu Kartes lietotāja identitāti vai mikroshēmā ietverto konta informāciju, vai abus (dažreiz mūsu materiālos saukta par „viedkarti", „EMV karti" vai „ICC" jeb „integrētās shēmas karti").

Pakalpojumu sniedzēji ir sertificētās starpniekiestādes, trešo pušu Starpniekiestādes, vārteju pakalpojumu sniedzēji, POS sistēmu integratori un jebkādi citi POS sistēmu Tirgotāju pakalpojumu sniedzēji vai citi maksājumu apstrādes risinājumi vai pakalpojumi.

Pašnovērtējuma anketa (SAQ) ir Payment Card Industry Security Standards Council, LLC izstrādāts pašnovērtējuma rīks, kura mērķis ir novērtēt un apliecināt atbilstību PCI DSS.

Paziņojuma datums ir datums, kurā American Express sniedz izdevējiem gala paziņojumu par Datu incidentu. Šis datums ir atkarīgs no datuma, kad American Express saņem gala izmeklēšanas ziņojumu vai iekšējo analīzi, un American Express nosaka šo datumu pēc saviem ieskatiem.

Pārdošanas punkta (POS) sistēma ir informācijas apstrādes sistēma vai iekārta, tajā skaitā termināls, personālais dators, elektroniskais kases aparāts, bezkontakta nolasītājs, maksājuma platforma vai process, kuru izmanto Tirgotājs, lai saņemtu autorizācijas vai iegūtu Darījuma datus, vai arī veiktu abas darbības.

PCI-apstiprināts nozīmē to, ka PIN ievades ierīce vai Maksājuma pieteikums (vai abi) parādās brīdī, kad tiek izmantoti PCI Security Standards Council, LLC kārtotajā apstiprināto uzņēmumu un pakalpojumu sniedzēju sarakstā, kas ir pieejams vietnē www.pcisecuritystandards.org.

PCI DSS ir Maksājumu karšu nozares datu drošības standarts, kas ir pieejams vietnē www.pcisecuritystandards.org.

PCI eksperts (PFI) ir persona, ko ir apstiprinājusi Maksājumu karšu nozares drošības standartu padome, LLC lai veiktu ekspertīzi par maksājumu kartes datu pārkāpumu vai apdraudējumu.

PCI PIN drošības prasības ir Maksājumu Karšu Nozares PIN Drošības prasības, kas ir pieejamas vietnē www.pcisecuritystandards.org.

PIN ievades ierīce ir lietota ar tādu nozīmi, kas šim terminam noteikta spēkā esošajā Maksājumu karšu nozares PIN darījumu drošības (PTS) mijiedarbības vietas (POI) modulārās drošības prasību terminu sarakstā, kas ir pieejams www.pcisecuritystandards.org.

Pircēja ierosinātas maksājuma (BIP) transakcijas ir maksājuma transakcija, kas iespējota, izmantojot maksājuma norādījuma datni, kas apstrādāta BIP.

Risku mazināšanas tehnoloģija ir tehnoloģiju risinājumi, kas uzlabo American Express Kartes lietotāja datu un Sensitīvo autentifikācijas datu drošību, kā to nosaka American Express. Lai kvalificētu tehnoloģiju kā Risku mazināšanas tehnoloģiju, jums jādemonstrē efektīva tehnoloģijas izmantošana atbilstoši tās izstrādes un paredzētajam mērķim. Piemēri: EMV, Divpunktu šifrēšana un tokenizācija.

Sensitīvi autentifikācijas dati ir lietoti ar nozīmi, kas šim terminam noteikta PCI DSS terminu sarakstā.

Skenēšanas atbilstības apliecinājums (AOSC) ir paziņojums par jūsu atbilstību PCI DSS, kas pamatojas uz interneta skenēšanu Payment Card Industry Security Standards Council, LLC noteiktajā veidā.

Starpniekiestāde ir Tirgotāju pakalpojumu sniedzējs, kurš veic autorizācijas un iesniegšanas apstrādi American Express tīklā.

Šifrēšanas atslēga (American Express Šifrēšanas atslēga) ir visas atslēgas, kuras tiek izmantotas Konta datu apstrādē, ģenerēšanā, ielādē un/vai aizsardzībā. Tas ietver, bet ne tikai, turpmāk minēto:

- Šifrēšanas atslēgas: zonas galvenās atslēgas (ZMK) un zonas PIN atslēgas (ZPK),
- drošās kriptogrāfijas ierīcēs izmantojamās galvenās atslēgas: lokālās galvenās atslēgas (LMK)
- Kartes drošības koda atslēgas (CSCK)
- PIN atslēgas: bāzes atvasinājuma atslēgas (BDK), PIN Šifrēšanas atslēga (PEK) un ZPK.

Tirgotājs ir tirgotājs un visas ar to saistītās personas, kas pieņem American Express Kartes atbilstoši Līgumam ar American Express vai ar to saistītajām personām.

Validācijas dokumentācija Atbilstības apliecinājums (AOC), kas sniegts saistībā ar Ikgadējo klātienes drošības novērtējumu, vai Pašnovērtējuma anketa (SAQ), Skenēšanas ziņojuma skenēšanas atbilstības apliecinājums (AOSC) un rezultātu kopsavilkums, kas sniegts saistībā ar tīkla skenēšanu reizi ceturksnī, vai Ikgadējā drošības tehnoloģiju uzlabojumu programmas atestācijā.