AMERICAN EXPRESS

Duomenų apsaugos užtikrinimo politika (DSOP)

AMERICAN EXPRESS

DSOP pakeitimų santrauka

Piktogramos

Svarbūs atnaujinimai išvardyti Pakeitimų santraukos lentelėje ir taip pat *DSOP* pažymėti pakeitimų juosta. Pakeitimų juosta – tai vertikali linija, paprastai kairėje paraštėje, kuria žymimas pridėtas arba pataisytas tekstas. Tik esminiai *DSOP* pakeitimai, galintys turėti poveikio Prekybininko veiklos procedūroms, yra nurodyti pakeitimų juosta kairėje paraštėje.

Pašalintas tekstas paryškinamas šiukšliadėžės piktograma, esančia paraštėje šalia bet kokio reikšmingo pašalinto teksto, įskaitant skirsnius, lenteles, pastraipas, pastabas ir punktus. Siekiant išvengti painiavos, šioje Pakeitimų santraukoje nuorodos į pašalintą tekstą pateikiamos naudojant ankstesnio leidinio skirsnių numeraciją.

Mėlynomis linijomis, ribojančiomis pastraipas, žymima konkrečiam regionui skirta informacija.

Pakeitimų santraukos lentelė

Svarbūs atnaujinimai išvardyti toliau pateiktoje lentelėje ir *DSOP* pažymėti pakeitimų juosta.

Skirsnis / poskirsnis	Pakeitimo aprašas
Šiam leidimui pakeitimų nėra.	

Skirsnis 1 Įvadas į DSOP ir apsaugos standartai

Kaip vartotojų apsaugos lyderė, „American Express“ jau daugybę metų deda visas pastangas siekdama užtikrinti Kortelės turėtojo duomenų ir Neskelbtinų tapatybės nustatymo duomenų apsaugą.

Duomenų apsaugos pažeidimai kenkia vartotojų, Prekybininkų, Paslaugų teikėjų ir kortelių išdavėjų interesams. Užtenka vieno incidento, kad būtų rimtai pakenkta įmonės reputacijai ir jos gebėjimui toliau efektyviai vykdyti savo veiklą. Šios problemos sprendimas taikant apsaugos užtikrinimo taisykles gali padėti įgyti klientų pasitikėjimą, padidinti pelningumą ir pagerinti įmonės reputaciją.

„American Express“ žino, kad Prekybininkams ir Paslaugų teikėjams (toliau kartu – jūs) rūpi tas pats, kas ir mums, todėl reikalauja, kad jūs prisiimdami atsakomybę laikytumėtės **jūsų** Sutartyje dėl „American Express®“ Kortelių priėmimo (Prekybininkų atveju) arba duomenų tvarkymo (Paslaugų teikėjų atveju) (toliau – **Sutartis**) numatytų duomenų apsaugos nuostatų ir šios Duomenų apsaugos užtikrinimo politikos (DSOP), kuri retkarčiais gali būti iš dalies keičiama. Šie reikalavimai taikomi visai jūsų įrangai, sistemoms ir tinklams (bei jų komponentams), kuriuose laikomi, tvarkomi arba perduodami Šifravimo raktai, Kortelės turėtojo duomenys ar Neskelbtini tapatybės nustatymo duomenys (arba bet koks šių duomenų derinys).

Čia neapibrėžti terminai, rašomi didžiąja raide, vartojami reikšmėmis, kurios jiems priskirtos žodyne, pateiktame šios politikos pabaigoje.

Duomenų apsaugos užtikrinimo politika (DSOP) – tai išsamių politikos reikalavimų rinkinys, skirtas apsaugoti Sąskaitų duomenis, kai tokie duomenys saugomi, tvarkomi ar perduodami.

„American Express“ reikalauja, kad visi Prekybininkai ir Paslaugų teikėjai atitiktų Mokėjimo kortelių pramonės duomenų apsaugos standartą (PCI DSS). Kaip šio reikalavimo dalis, jūs ir jūsų Apsaugotosios šalys privalo:

- laikyti Kortelės turėtojo duomenis tik tam, kad pagal šią Sutartį ir laikydamiesi jos reikalavimų atliktų Sandorius su „American Express“ kortelėmis;
- laikytis jūsų Kortelės turėtojo duomenų ir Neskelbtinų tapatybės nustatymo duomenų tvarkymui, laikymui ar perdavimui taikomo naujausio Mokėjimo kortelių pramonės duomenų apsaugos standarto (angl. „Payment Card Industry Data Security Standard“, PCI DSS) ir kitų Mokėjimo kortelių pramonės apsaugos standartų tarybos (angl. „Payment Card Industry Security Standards Council“, PCI SSC) reikalavimų versijos ne vėliau kaip nuo jos įsigaliojimo dienos;
- užtikrinti, kad diegiant arba keičiant technologijas, skirtas duomenims saugoti, tvarkyti arba perduoti, būtų naudojami PCI patvirtinti produktai.

Privalote užtikrinti visų „American Express“ Mokesčių įrašų ir Kredito įrašų, laikomų pagal Sutarties reikalavimus, apsaugą taip, kaip numatyta šiose duomenų apsaugos nuostatose; tokius įrašus galite naudoti tik Sutarties tikslais ir privalote atitinkamai juos apsaugoti. Finansiškai ir kitaip įsipareigojate „American Express“ užtikrinti, kad jūsų Apsaugotosios šalys laikosi šių duomenų apsaugos nuostatų (ir ne tik tam, kad parodytumėte, jog jūsų Apsaugotosios šalys laikosi šios politikos, kaip tai numatyta Skirsnis 2, „PCI DSS atitikties programa (svarbus periodinis jūsų sistemų atitikties patvirtinimas)“, nebent jame būtų numatyta kitaip). Išsamios informacijos apie PCI standartus ir kaip laikytis jų reikalavimų galima rasti svetainėje www.pcisecuritystandards.org.

Skirsnis 2 PCI DSS atitikties programa (svarbus periodinis jūsų sistemų atitikties patvirtinimas)

Kiekvienais metais ir kas 90 dienų pagal PCI DSS, kaip nurodyta toliau, privalote toliau nurodytais veiksmais patvirtinti savo ir jūsų Franšizės turėtojų įrangos, sistemų ir (arba) tinklų (bei jų komponentų), kuriuose laikomi, tvarkomi arba perduodami Kortelės turėtojo duomenys arba Neskelbtini tapatybės nustatymo duomenys, atitiktį.

Tam būtina atlikti 4 veiksmus:

- Veiksmas 1: Pagal šią politiką dalyvauti „American Express“ PCI atitikties programoje.
- Veiksmas 2: Suprasti savo Prekybininko / Paslaugų teikėjo lygį ir Patvirtinimo dokumentų reikalavimus.

- Veiksmas 3: Užpildyti Patvirtinimo dokumentus, kuriuos reikia nusiųsti „American Express“.
- Veiksmas 4: Nusiųsti Patvirtinimo dokumentus „American Express“.

Veiksmas 1: Pagal šią politiką dalyvauti „American Express“ atitikties programoje

1 lygio Prekybininkai, 2 lygio Prekybininkai ir visi Paslaugų teikėjai, kaip aprašyta toliau, privalo dalyvauti Programoje pagal šią politiką. „American Express“ savo nuožiūra gali paskirti konkrečius 3 ir 4 lygio Prekybininkus dalyvauti Programoje pagal šią politiką.

Prekybininkas ir Paslaugų teikėjai, kurie turi dalyvauti Programoje, turi užsiregistruoti „American Express“ pasirinkto Programos administratoriaus Portale per nustatytus terminus.

- Privalote sutikti su visomis pagrįstomis sąlygomis, susijusiomis su Portalo naudojimu.
- Portale turite paskirti bent vieną kontaktinį asmenį duomenų apsaugos klausimais ir pateikti tikslią informaciją apie jį. Reikalinga informacija:
  - Vardas ir pavardė
  - El. pašto adresas
  - Telefono numeris
  - Fizinis pašto adresas
- Pasikeitus paskirtojo kontaktinio asmens duomenų apsaugos klausimais kontaktinei informacijai Portale turite pateikti atnaujintą arba naują kontaktinę informaciją.
- Privalote užtikrinti, kad jūsų sistemos būtų atnaujintos ir leistų palaikyti paslaugų ryšius iš Portalo paskirtojo domeno.

Jei nepateiksite ar nepalaikysite aktualios duomenų apsaugos kontaktinės informacijos arba neįjungsite el. pašto pranešimų, tai neturės įtakos mūsų teisėms apskaičiuoti mokesčius.

Veiksmas 2: Suprasti savo Prekybininko / Paslaugų teikėjo lygį ir Patvirtinimo dokumentų reikalavimus

Pagal Sandorių su „American Express“ kortelėmis kiekį Prekybininkai skirstomi į keturis lygius, o Paslaugų teikėjai – į du lygius.

- Prekybininkams tai yra jų Įstaigų pateikti kiekiai, kurie pasiekia aukščiausią „American Express“ Prekybininko sąskaitos lygį.*
- Paslaugų teikėjų atveju tai yra Paslaugų teikėjo ir Subjektų, kuriems teikiate paslaugas, pateiktų kiekių suma.

Pirkėjo inicijuoto mokėjimo (angl. „Buyer Initiated Payments“, BIP) Sandoriai neįtraukiami į „American Express“ kortelių Sandorių kiekį, pagal kurį nustatomas Prekybininko lygis ir jo statuso patvirtinimo reikalavimai. Pateksite į vieną iš Prekybininkų lygių, nurodytų A-1 lentelė: Prekybininkų arba Paslaugų teikėjų lygiai.

* Franšizės davėjų atveju skaičiuojamas ir Franšizės gavėjų įstaigų kiekis. Franšizės davėjai, kurie reikalauja, kad jų Franšizės gavėjai naudotų nurodytą Pardavimo vietos (angl. „Point of Sale“, POS) sistemą arba Paslaugų teikėją, taip pat turi pateikti atitinkamų Franšizės gavėjų patvirtinimo dokumentus.

A-1 lentelė: Prekybininkų arba Paslaugų teikėjų lygiai

Prekybininko lygis	Metinis „American Express“ Sandorių skaičius
1 lygio Prekybininkas	2,5 mln. ar daugiau „American Express“ kortelių Sandorių per metus; arba bet kuris Prekybininkas, kurį „American Express“ savo nuožiūra priskiria 1 lygiui.
2 lygio Prekybininkas	Nuo 50 000 iki mažiau kaip 2,5 mln. „American Express“ kortelių Sandorių per metus.
3 lygio Prekybininkas	Nuo 10 000 iki mažiau kaip 50 000 mln. „American Express“ kortelių Sandorių per metus.
4 lygio Prekybininkas	Mažiau nei 10 000 „American Express“ kortelių Sandorių per metus.
Paslaugų teikėjo lygis	**Metinis „American Express“ Sandorių skaičius**
1 lygio Paslaugų teikėjas	2,5 mln. ar daugiau „American Express“ kortelių Sandorių per metus; arba bet kuris Paslaugų teikėjas, kurį „American Express“ savo nuožiūra priskiria 1 lygiui.
2 lygio Paslaugų teikėjas	Mažiau kaip 2,5 mln. „American Express“ kortelių Sandorių per metus arba bet kuris Paslaugų teikėjas, kurio „American Express“ nepriskyrė 1 lygiui.

Prekybininkų patvirtinimo dokumentų reikalavimai

Prekybininkai (ne Paslaugų teikėjai) turi keturias galimas Prekybininkų lygio klasifikacijas. Nustatę Prekybininko lygį iš A-1 lentelė: Prekybininkų arba Paslaugų teikėjų lygiai (pateikta pirmiau), žr. A-2 lentelė: „Prekybininkų Patvirtinimo dokumentai“ ir nustatykite patvirtinimo dokumentų reikalavimus.

A-2 lentelė: Prekybininkų Patvirtinimo dokumentai

Prekybininko lygis / metinis „American Express“ Sandorių skaičius	Ataskaita apie atitikties patvirtinimo reikalavimų laikymąsi (ROC AOC)	Atitikties patvirtinimo įsivertinimo anketa (SAQ AOC) IR ketvirtinė išorinio tinklo pažeidžiamumo patikra (toliau – Patikra)	Apsaugos technologijų tobulinimo programos (STEP) reikalavimus atitinkančių Prekybininkų atestacija
1 lygis / 2,5 mln. arba daugiau	Privaloma	Netaikoma	Neprivaloma su „American Express“ patvirtinimu (pakeičia ROC)
2 lygis / nuo 50 000 iki mažiau kaip 2,5 mln.	Neprivaloma	SAQ AOC privaloma (jei nepateikta ROC AOC); patikra privaloma su tam tikrų rūšių SAQ	Neprivaloma su „American Express“ patvirtinimu* (pakeičia SAQ ir tinklo patikrą arba ROC)
3 lygis** / nuo 10 000 iki mažiau kaip 50 000	Neprivaloma	SAQ AOC neprivaloma (privaloma, jei reikalauja „American Express“); patikra privaloma su tam tikrų rūšių SAQ	Neprivaloma su „American Express“ patvirtinimu* (pakeičia SAQ ir tinklo patikrą arba ROC)
4 lygis** / mažiau kaip 10 000	Neprivaloma	SAQ AOC neprivaloma (privaloma, jei reikalauja „American Express“); patikra privaloma su tam tikrų rūšių SAQ	Neprivaloma su „American Express“ patvirtinimu* (pakeičia SAQ ir tinklo patikrą arba ROC)

* **Pastaba.** „American Express“ PCI komanda peržiūrės prašymą ir atitiktį reikalavimams bei patvirtins, ar jums gali būti taikoma STEP programa. Susisiekite su savo Klientų vadybininku ir (arba) rašykite AXPPCIComplianceProgram@aexp.com, kad patikrintumėte atitikimą reikalavimams.

**Kad nekiltų jokių abejonių, reikia pažymėti, jog 3 ir 4 lygio Prekybininkai neprivalo pateikti Patvirtinimo dokumentų, nebent to savo nuožiūra reikalautų „American Express“, tačiau jie vis tiek privalo laikytis visų kitų šios Duomenų apsaugos užtikrinimo politikos nuostatų ir prisiimti jose numatytą atsakomybę.

„American Express“ pasilieka teisę tikrinti jūsų PCI patvirtinimo dokumentų išbaigtumą, tikslumą ir tinkamumą. Šiam tikslui pagrįsti „American Express“ gali pareikalauti, kad pateiktumėte papildomus patvirtinamuosius dokumentus įvertinimui. Be to, „American Express“ turi teisę reikalauti, kad pasitelktumėte „PCI Security

Standards Council“ patvirtintą Kvalifikuotą saugumo vertintoją (QSA) ar PCI teisminės ekspertizės specialistą (PFI).

Paslaugų teikėjų Patvirtinimo dokumentų reikalavimai

Paslaugų teikėjai (ne Prekybininkai) turi dvi galimas Lygio klasifikacijas. Nustatę Paslaugų teikėjo lygį iš A-1 lentelė: Prekybininkų arba Paslaugų teikėjų lygiai (pateikta pirmiau), žr. A-3 lentelė: „Paslaugų teikėjų Patvirtinimo dokumentai“ ir nustatykite patvirtinimo dokumentų reikalavimus.

Paslaugų teikėjai negali dalyvauti STEP programoje.

A-3 lentelė: Paslaugų teikėjų Patvirtinimo dokumentai

Lygis	Patvirtinimo dokumentai	Reikalavimas
1	Metinė ataskaita apie atitikties patvirtinimo reikalavimų laikymąsi (ROC AOC)	Privaloma
2	Metinė SAQ D (Paslaugų teikėjas) ir Ketvirtinė tinklo saugumo patikra arba Metinė ataskaita apie atitikties patvirtinimo reikalavimų laikymąsi (ROC AOC), jei pageidaujama	Privaloma

Paslaugų teikėjams taip pat rekomenduojama laikytis PCI nurodytų subjektų papildomo patvirtinimo tvarkos.

Apsaugos technologijų tobulinimo programa (STEP)

Prekybininkams, atitinkantiems PCI DSS reikalavimus, „American Express“ savo nuožiūra gali suteikti teisę dalyvauti „American Express“ STEP (angl. „Security Technology Enhancement Programme“) programoje, jeigu jie savo Kortelių duomenų tvarkymo aplinkoje įrengia tam tikras papildomas apsaugos technologijas. STEP taikoma tik tuo atveju, jeigu per pastaruosius 12 mėnesių Prekybininkas nepatyrė jokių Duomenų saugumo pažeidimų ir jeigu 75 % visų Prekybininko Sandorių buvo vykdomi naudojant šių patobulintų apsaugos variantų derinį:

- **EMV, „EMV Contactless“ arba „Digital Wallet“** – aktyviu Lustinių kortelių nuskaitymo aparatu su galiojančiu ir nepasenusiu EMVCo (www.emvco.com) sertifikatu, kuriuo galima atlikti AEIPS atitinkančius Lustinių kortelių Sandorius. (JAV Prekybininkai turi nurodyti ir bekontakčius Sandorius)
- **Tiesioginis šifravimas** (angl. „Point-to-Point Encryption“, P2PE) – Sandoriai Prekybininko duomenų tvarkytojui siunčiami naudojant PCI SSC arba QSA patvirtintą Tiesioginio šifravimo sistemą
- **Pakeista atpažinimo ženklu** – įdiegtas atpažinimo ženklų naudojimo sprendimas turi:
  - atitikti EMVCo specifikacijas;
  - būti apsaugotas, apdorojamas, laikomas, perduotas ir visiškai tvarkomas PCI reikalavimus atitinkančio trečiųjų šalių paslaugų teikėjo;
  - Atpažinimo ženklas negali būti atstatytas, kad Prekybininkui būtų atskleisti neužmaskuoti Pirminiai sąskaitų numeriai (PAN).

Prekybininkams, turintiems teisę dalyvauti STEP, taikomi mažiau griežti PCI Patvirtinimo dokumentų reikalavimai, kaip nurodyta Veiksmas 3: „Užpildyti Patvirtinimo dokumentus, kuriuos reikia nusiųsti „American Express““.

Veiksmas 3: Užpildyti Patvirtinimo dokumentus, kuriuos reikia nusiųsti „American Express“

Skirtingų lygių Prekybininkai ir Paslaugų teikėjai privalo pateikti toliau nurodytus dokumentus, kaip nurodyta pirmiau pateiktoje A-2 lentelė: „Prekybininkų Patvirtinimo dokumentai“ ir A-3 lentelė: „Paslaugų teikėjų Patvirtinimo dokumentai“.

Atitinkamam vertinimo tipui turite pateikti Atitikties patvirtinimą (AOC). AOC yra jūsų atitikties statuso deklaracija, todėl ją turi pasirašyti ir nurodyti datą atitinkamo lygio organizacijos vadovai.

Be AOC, „American Express“ gali pareikalauti, kad pateiktumėte visapusiško vertinimo kopiją ir, mūsų nuožiūra, papildomus patvirtinamuosius dokumentus, įrodančius atitiktį PCI DSS reikalavimams. Šie Patvirtinimo dokumentai užpildomi jūsų sąskaita.

Ataskaita apie atitikties patvirtinimo reikalavimų laikymąsi (ROC AOC) – (kasmetinis reikalavimas) – Ataskaitoje apie atitiktį pateikiami išsamaus jūsų įrangos, sistemų ir tinklų (ir jų sudedamųjų dalių), kur saugomi, tvarkomi arba perduodami Kortelių turėtojų duomenys arba Neskelbtini tapatybės nustatymo duomenys (arba ir vieni, ir kiti), patikrinimo vietoje rezultatai. Galimos dvi versijos: viena Prekybininkams, o kita – Paslaugų teikėjams. Ataskaitą apie atitiktį turi parengti:

- QSA, arba
- Vidaus saugumo vertintojas (ISA), o patvirtinti turi jūsų generalinis direktorius, finansų direktorius, informacijos apsaugos skyriaus vadovas arba direktorius

ROC AOC turi būti pasirašyta ir datuota QSA arba ISA ir įgalioto lygio vadovo jūsų organizacijoje ir pateikta „American Express“ bent kartą per metus.

Atitikties patvirtinimo įsivertinimo anketa (SAQ AOC) – (kasmetinis reikalavimas) – Įsivertinimo anketos leidžia patikrinti įrangą, sistemas ir tinklus (ir jų sudedamąsias dalis), kur saugomi, tvarkomi arba perduodami Kortelių turėtojų duomenys arba Neskelbtini tapatybės nustatymo duomenys (arba ir vieni, ir kiti). Yra daugybė SAQ variantų. Jūs pasirinksite vieną ar kelis pagal savo Kortelės turėtojo duomenų aplinką.

SAQ gali užpildyti jūsų Įmonės darbuotojai, turintys kvalifikaciją tiksliai ir išsamiai atsakyti į klausimus, arba galite pasitelkti į pagalbą QSA. SAQ AOC turi būti pasirašyta ir datuota įgalioto lygio vadovo jūsų organizacijoje ir pateikta „American Express“ bent kartą per metus.

Aprobuotosios saugumo patikros įmonės išorinio tinklo pažeidžiamumo patikros suvestinė (ASV saugumo patikra) – (90 dienų reikalavimas) – Išorinio pažeidžiamumo patikra – tai nuotolinis testas, padedantis nustatyti galimas silpnąsias vietas, pažeidžiamumus ir neteisingą jūsų Kortelių turėtojų duomenų aplinkos su internetu susijusių komponentų konfigūraciją (pvz., interneto svetainių, taikomųjų programų, interneto serverių, pašto serverių, viešai prieinamų domenų ar pagrindinių kompiuterių).

ASV patikrą turi atlikti Aprobuotoji saugumo patikros įmonė (ASV).

Jei reikalaujama pagal SAQ, bent kartą per 90 dienų „American Express“ turi būti pateikta ASV saugumo atitikties patvirtinimo ataskaita (AOSC) arba suvestinė, įskaitant patikrintų objektų skaičių, patvirtinimą, kad rezultatai atitinka PCI DSS patikros procedūras, ir ASV užpildytą atitikties statusą.

Jei pateikiate ROC AOC arba STEP, neprivalote pateikti AOSC arba ASV patikros suvestinės, išskyrus atvejus, kai to konkrečiai prašoma. Kad nekiltų abejonių, saugumo patikros yra privalomos, jeigu to reikalaujama atitinkamoje SAQ.

STEP atestacijos patvirtinimo dokumentai (STEP) – (kasmetinis reikalavimas) – STEP siūloma tik Prekybininkams, kurie atitinka pirmiau pateikto Veiksmas 2: „Suprasti savo Prekybininko / Paslaugų teikėjo lygį ir Patvirtinimo dokumentų reikalavimus“ kriterijus. Jei jūsų įmonė atitinka reikalavimus, privalote kasmet atlikti atestaciją ir pateikti „American Express“ STEP atestacijos formą. Kasmetinę STEP atestacijos formą galite atsisiųsti iš Portalo. Taip pat galite susisiekti su savo Klientų vadybininku arba parašyti „American Express“ adresu AXPPCICompliceProgram@aexp.com.

PCI DSS reikalavimų neatitikimas – (kasmetinis, 90 dienų ir (arba) ad hoc reikalavimas) – Jei neatitinkate PCI DSS reikalavimų, tuomet turite pateikti PCI prioritetinio metodo priemonės (PAT) suvestinę (galima atsisiųsti iš „PCI Security Standards Council“ interneto svetainės).

PAT suvestinėje turite nurodyti datą, iki kurios planuojate padėtį ištaisyti, tačiau ji turi būti ne vėliau kaip 12 (dvylika) mėnesių nuo dokumento užpildymo, kad įvykdytumėte atitikties reikalavimus. Periodiškai informuosite „American Express“ apie savo daromą pažangą siekiant vėl užtikrinti atitiktį (1, 2, 3 ir 4 lygio Prekybininkai; visi Paslaugų teikėjai). Taisomieji veiksmai, reikalingi atitikčiai PCI DSS užtikrinti, turi būti atlikti jūsų sąskaita.

American Express“ netaikys mokesčių už atitikties neužtikrinimą iki trūkumų pašalinimo datos. Pagal A-4 lentelė: „Mokestis už atitikties neužtikrinimą“, jūs esate atsakingi „American Express“ už visas prievoles atlyginti Duomenų saugumo pažeidimo žalą ir privalote laikytis visų kitų šios politikos nuostatų.

„American Express“ savo nuožiūra pasilieka teisę taikyti mokesčius už atitikties neužtikrinimą, jeigu:

- pagal šiame skirsnyje nurodytus reikalavimus nepateiktas PCI prioritetinio metodo šablonas;
- nesilaikyta PCI prioritetinio metodo šablone dėl neatitikties būsenos nurodytų taisomųjų veiksmų;
- nebuvo įvykdyti PCI prioritetinio metodo šablono dėl neatitikties būsenos reikalavimai arba
- privalomi atitikties dokumentai nebuvo pateikti „American Express“ iki nustatyto termino arba pareikalavus.

Prekybininkams / Paslaugų teikėjams, kurie nesilaiko Veiksmas 2: „Suprasti savo Prekybininko / Paslaugų teikėjo lygį ir Patvirtinimo dokumentų reikalavimus“ pateiktų reikalavimų, gali būti taikomi mokesčiai, kaip nurodyta Veiksmas 4: „Nusiųsti Patvirtinimo dokumentus „American Express“ iki nurodyto termino“.

Kad nekiltų jokių abejonių, reikia pažymėti, jog Prekybininkai, neatitinkantys PCI DSS reikalavimų, negali dalyvauti STEP programoje.

Veiksmas 4: Nusiųsti Patvirtinimo dokumentus „American Express“ iki nurodyto termino

Visi Prekybininkai ir Paslaugų teikėjai, turintys dalyvauti Programoje, privalo „American Express“ iki atitinkamų terminų pateikti Patvirtinimo dokumentus, kurie Veiksmas 2: „Suprasti savo Prekybininko / Paslaugų teikėjo lygį ir Patvirtinimo dokumentų reikalavimus“ lentelėse pažymėti kaip „privalomi“.

Patvirtinimo dokumentus „American Express“ turite pateikti naudodamiesi „American Express“ pasirinkto Programos administratoriaus pateiktu Portalu. Pateikdami Patvirtinimo dokumentus „American Express“ patvirtinate ir garantuojate, kad toliau nurodyti duomenys yra teisingi (kiek tai įmanoma):

- jūsų vertinimas buvo išbaigtas ir kruopštus;
- PCI DSS būsena tiksliai nurodyta pildant ar pateikiant Atitikties patvirtinimą (AOC) arba PCI prioritetinio metodo priemonės (PAT) suvestinę dėl neatitikties;
- esate įgaliotas atskleisti čia pateiktą informaciją ir pateikiate „American Express“ Patvirtinimo dokumentus nepažeisdamas jokios kitos šalies teisių.

Mokesčiai už atitikties neužtikrinimą ir Sutarties nutraukimas

„American Express“ turi teisę taikyti jums mokesčius už atitikties neužtikrinimą ir nutraukti Sutartį, jeigu neįvykdysite šių reikalavimų arba iki nurodyto termino nepateiksite „American Express“ privalomų Patvirtinimo dokumentų. „American Express“ praneš duomenų apsaugos kontaktiniam asmeniui apie kiekvienų metų ir ketvirčio ataskaitų atitinkamus pateikimo terminus.

A-4 lentelė: Mokestis už atitikties neužtikrinimą

Aprašas*	1 lygio Prekybininkas arba 1 lygio Paslaugų teikėjas	2 lygio Prekybininkas arba 2 lygio Paslaugų teikėjas	3 lygio arba 4 lygio Prekybininkas
Jeigu Patvirtinimo dokumentai nebus gauti iki pirmojo termino, bus paskirtas mokestis už atitikties neužtikrinimą.	25 000 JAV dol.	5 000 JAV dol.	50 JAV dol.
Jeigu Patvirtinimo dokumentai nebus gauti iki antrojo termino, bus paskirtas papildomas mokestis už atitikties neužtikrinimą.	35 000 JAV dol.	10 000 JAV dol.	100 JAV dol.
Jeigu Patvirtinimo dokumentai nebus gauti iki trečiojo termino, bus paskirtas papildomas mokestis už atitikties neužtikrinimą. **PASTABA.** Mokesčiai už atitikties neužtikrinimą bus taikomi tol, kol nebus pateikti Patvirtinimo dokumentai.	45 000 JAV dol.	15 000 JAV dol.	250 JAV dol.

* Atitikties neužtikrinimo mokesčiai bus apskaičiuojami Vietine valiuta.

* Netaikoma Argentinai.

Jei jūsų PCI DSS atitikties dokumentų įsipareigojimai neįvykdomi, „American Express“ turi teisę taikyti sukauptus mokesčius už atitikties neužtikrinimą, sulaikyti mokėjimus ir (arba) nutraukti Sutartį.

Skirsnis 3 Duomenų saugumo pažeidimų valdymo įsipareigojimai

Privalote neatidėliodami ir ne vėliau kaip per septyniasdešimt dvi (72) valandas pranešti „American Express“ apie išsiaiškintą Duomenų saugumo pažeidimą.

Tam kreipkitės į „American Express“ įmonių incidentų sprendimų programą (angl. „Enterprise Incident Response Programme“) (*EIRP*) nemokamu telefonu +1 (888) 732-3750 arba +1 (602) 537-3021 arba el. paštu EIRP@aexp.com. Turite paskirti kontaktinį asmenį bendravimui dėl Duomenų saugumo pažeidimų. Taip pat:

- Privalote atlikti kiekvieno Duomenų saugumo pažeidimo kruopštų tyrimą ir skubiai pateikti „American Express“ visus Pažeistų kortelių numerius. „American Express“ turi teisę atlikti savarankišką vidinį tyrimą, kad išsiaiškintų visus su Duomenų saugumo pažeidimu susijusius duomenis.

Duomenų saugumo pažeidimams, susijusiems su mažiau kaip 10 000 unikalių Kortelių numerių, tyrimo suvestinė turi būti pateikta „American Express“ per dešimt (10) darbo dienų nuo jo pabaigos.

- Tyrimo suvestinėse turi būti pateikta ši informacija: pažeidimo suvestinė, paveiktos (-ų) aplinkos (-ų) aprašymas, įvykių chronologija, pagrindinės datos, poveikio ir duomenų poveikio informacija, apribojimo ir

taisomieji veiksmai ir patvirtinimas, kad nėra jokių požymių, kad kyla pavojus papildomiems „American Express“ duomenims.

Duomenų saugumo pažeidimams, susijusiems su 10 000 ar daugiau unikalių Kortelių numerių, privalote kreiptis į PCI PFI, kad jis atliktų tokį tyrimą per penkias (5) dienas nuo tada, kai buvo nustatytas Duomenų saugumo pažeidimas.

- Neredaguota ekspertizės ataskaita turi būti pateikta „American Express“ per dešimt (10) darbo dienų nuo ekspertizės pabaigos.
- Ekspertizės ataskaitos turi būti parengtos naudojant galiojantį pažeidimo galutinės ekspertizės ataskaitos šabloną, kurį galima gauti iš PCI. Ataskaitą turi sudaryti ekspertiniai vertinimai, atitikties vertinimai ir visa kita su Duomenų saugumo pažeidimu susijusi informacija; turi būti nurodyta Duomenų saugumo pažeidimo priežastis; turi būti nurodyta, ar Duomenų saugumo pažeidimo metu jūs laikėtės PCI DSS; taip pat turi būti patvirtintas jūsų gebėjimas ateityje išvengti Duomenų saugumo pažeidimų (i) pateikiant visų PCI DSS trūkumų šalinimo planą ir (ii) dalyvaujant „American Express“ atitikties programoje (aprašytoje toliau). „American Express“ prašymu turite pateikti Kvalifikuoto saugumo vertintojo (angl. „Qualified Security Assessor“, QSA) patvirtinimą, kad nustatyti trūkumai pašalinti.

Nepaisant Skirsnis 3, „Duomenų saugumo pažeidimų valdymo įsipareigojimai“:

- „American Express“ gali savo nuožiūra pareikalauti, kad jūs įtrauktumėte PFI Duomenų saugumo pažeidimui tirti, kai Duomenų saugumo pažeidimai, susiję su mažiau kaip 10 000 unikalių Kortelių numerių arba kai per 12 mėnesių laikotarpį buvo nustatyta daug pažeidimų. Toks tyrimas turi atitikti Skirsnis 3, „Duomenų saugumo pažeidimų valdymo įsipareigojimai“ reikalavimus ir turi būti atliktas per „American Express“ nustatytą laiką.
- „American Express“ gali savo nuožiūra atskirai kreiptis į PFI bet kokio Duomenų saugumo pažeidimo tyrimui atlikti ir reikalauti jūsų padengti tokio tyrimo išlaidas.

Turite įvertinti Duomenų saugumo pažeidimą pagal visame pasaulyje taikomus pranešimo apie duomenų saugumo pažeidimą įstatymus ir, jei manote, kad tai būtina, pranešti atitinkamoms reguliavimo institucijoms ir nukentėjusiems Kortelių naudotojams pagal pranešimo apie duomenų saugumo pažeidimą įstatymus. Jei nustatėte, kad už pranešimą apie Duomenų saugumo pažeidimą atsakingas jūsų Paslaugų teikėjas arba kitas subjektas, turite informuoti tokį Paslaugų teikėją arba subjektą apie jo pareigą įvertinti savo pranešimo prievoles pagal taikomus pranešimo apie duomenų saugumo pažeidimą įstatymus. Sutinkate gauti raštišką „American Express“ sutikimą prieš nurodydami ar įvardydami „American Express“ bet kokiuose Kortelės naudotojams skirtuose pranešimuose apie Duomenų saugumo pažeidimą. Jūs sutinkate bendradarbiauti su „American Express“ teikiant informaciją ir sprendžiant visas problemas, kylančias dėl Duomenų saugumo pažeidimo, įskaitant teikti „American Express“ visą aktualią informaciją (bei gauti visus reikalingus atsisakymus), reikalingą norint patvirtinti jūsų gebėjimą užkirsti kelią Duomenų saugumo pažeidimams ateityje laikantis Sutarties nuostatų.

Nepaisant Sutartyje numatytų priešingų konfidencialumo įsipareigojimų, „American Express“ turi teisę atskleisti informaciją apie bet kokius Duomenų saugumo pažeidimus „American Express“ Kortelių naudotojams, išdavėjams, kitiems „American Express“ tinklo dalyviams bei viešai, jei to reikalauja taikomi teisės aktai, teismo, administracinis ar reguliavimo nurodymas, dekretas, teismo šaukimas, prašymas ar kitas procesas, siekiant sumažinti sukčiavimo ar kitokios žalos riziką, arba tiek, kiek reikia „American Express“ tinklo veiklai užtikrinti.

Ką daryti įvykus Duomenų saugumo pažeidimui?

Atlikite šiuos žingsnius, jei nustatėte Duomenų saugumo pažeidimą vykdant savo veiklą.

1 žingsnis

Užpildykite Prekybininko Duomenų saugumo pažeidimo pradinę pranešimo formą ir nusiųskite EIRP@aexp.com per 72 valandas nuo Duomenų saugumo pažeidimo nustatymo.

2 žingsnis

Atlikite išsamų tyrimą; tam gali prireikti Mokėjimo kortelių pramonės (angl. „Payment Card Industry“, PCI) teisminės ekspertizės specialisto.

3 žingsnis

Nedelsiant pateikite mums visus „American Express®“ kortelių, dėl kurių įvyko pažeidimas, numerius.

4 žingsnis

Bendradarbiaukite su mumis, kad padėtumėte išspręsti problemas, kylančias dėl Duomenų saugumo pažeidimo.

Žr. Skirsnis 3, „Duomenų saugumo pažeidimų valdymo įsipareigojimai“ dėl detalesnės informacijos apie Duomenų saugumo pažeidimų valdymoįsipareigojimus.

Turite daugiau klausimų?

JAV: (888) 732-3750 (nemokamas)

Tarptautinis: +1 (602) 537-3021

EIRP@aexp.com

Skirsnis 4 Prievolė atlyginti Duomenų saugumo pažeidimo žalą

Jūsų prievolė „American Express“ atlyginti žalą, patirtą dėl Duomenų saugumo pažeidimo, nustatoma „American Express“ neatsisakant jokių kitų teisių ir teisių gynimo priemonių, numatytų Skirsnis 4, „Prievolė atlyginti Duomenų saugumo pažeidimo žalą“. Be prievolių atlyginti žalą (jei tokių yra), jums gali būti taikomas mokestis už Duomenų saugumo pažeidimą, kaip aprašyta toliau Skirsnis 4, „Prievolė atlyginti Duomenų saugumo pažeidimo žalą“.

Privalote sumokėti „American Express“ 5 JAV dol. kompensaciją už kiekvieną sąskaitos numerį šių Duomenų saugumo pažeidimų atveju:

- 10 000 ar daugiau „American Express“ Kortelių numerių su:
  - Neskelbtinais tapatybės nustatymo duomenimis, arba
  - Galiojimo laiku

„American Express“ neprašys jūsų atlyginti žalos dėl Duomenų saugumo pažeidimų, susijusių su:

- mažiau nei 10 000 „American Express“ kortelių numerių, arba
- daugiau nei 10 000 „American Express“ kortelių numerių, jei tenkinamos šios sąlygos:
  - pranešėte „American Express“ apie Duomenų saugumo pažeidimą pagal Skirsnis 3, „Duomenų saugumo pažeidimų valdymo įsipareigojimai“,
  - duomenų saugumo pažeidimo metu laikėtės PCI DSS standarto (tai turi būti nustatyta PFI atliktame Duomenų saugumo pažeidimo tyrime), ir
  - Duomenų saugumo pažeidimas įvyko ne dėl jūsų ar Apsaugotųjų šalių netinkamų veiksmų.

Nepaisant ankstesnių Skirsnis 4, „Prievolė atlyginti Duomenų saugumo pažeidimo žalą“ punktų, jei nesilaikote bet kurio įsipareigojimo, numatyto Skirsnis 3, „Duomenų saugumo pažeidimų valdymo įsipareigojimai“, už kiekvieną Duomenų saugumo pažeidimą, neatsižvelgiant į „American Express“ Kortelių numerių skaičių, privalote sumokėti „American Express“ mokestį už Duomenų saugumo pažeidimą, kuris siekia iki 100 000 JAV dol. (sumą savo nuožiūra nustato „American Express“). Kad nekiltų abejonių, bendras už Duomenų saugumo pažeidimą mokėtinas mokestis negali viršyti 100 000 JAV dol.

„American Express“ skaičiavimuose neatsižvelgs į „American Express“ Kortelių sąskaitos numerius, kurie dalyvavo ankstesnėje pretenzijoje dėl Duomenų saugumo pažeidimo, pateiktą per dvylika (12) mėnesių iki Pranešimo dienos. Visi „American Express“ skaičiavimai pagal šią metodiką yra galutiniai.

„American Express“ gali pateikti sąskaitą už visą jūsų įsipareigojimų atlyginti žalą dėl Duomenų saugumo pažeidimo sumą arba išskaityti šią sumą iš „American Express“ mokėjimų jums (arba nurašyti šią sumą iš jūsų Banko sąskaitos) pagal Sutartį.

Čia numatyta jūsų prievolė atlyginti žalą, patirtą dėl Duomenų saugumo pažeidimų, pagal Sutartį nelaikoma atsitiktine, netiesiogine, hipotetine, logiškai išplaukiančia, ypatinga, baudžiamąja arba baudine žala su sąlyga, kad toks įsipareigojimas neapima žalos, kurios pobūdis yra arba kuri yra susijusi su prarastu pelnu ar pajamomis, prestižo sumažėjimu ar verslo galimybių praradimu.

„American Express“ gali savo nuožiūra sumažinti Prekybininkų žalos atlyginimo prievolę dėl Duomenų saugumo pažeidimų tik jeigu tenkinamos visos šios sąlygos:

- iki Duomenų saugumo pažeidimo ir visą Duomenų saugumo pažeidimo laikotarpį buvo naudojamos tinkamos Rizikos mažinimo technologijos,
- buvo atliktas kruopštus tyrimas pagal PFI programą (nebent raštu iš anksto būtų susitarta kitaip),
- ekspertizės ataskaitoje aiškiai nurodyta, kad Duomenų saugumo pažeidimo metu Rizikos mažinimo technologijos buvo naudotos duomenims tvarkyti, laikyti ir (arba) perduoti, ir
- jūs nelaikote (ir Duomenų saugumo pažeidimo laikotarpiu nelaikėte) Neskelbtinų tapatybės nustatymo duomenų arba kitų Kortelės turėtojo duomenų, kurie nebuvo padaryti nenuskaitomi.

Jeigu yra prievolės nuolaidos galimybė, tokia nuolaida (atmetus už Duomenų saugumo pažeidimą mokėtinus mokesčius) nustatoma taip:

A-5 lentelė: Žalos atlyginimo prievolės nuolaidos sąlygos

Žalos atlyginimo prievolės nuolaida	Privalomos sąlygos
Standartinė nuolaida: 50 %	>75 % visų Sandorių atliekama su Lustinių kortelių nuskaitymo aparatais[1] ARBA
	>75 % Prekybininko prekybos vietų naudoja Rizikos mažinimo technologiją[2]
Padidinta nuolaida: 75–100 %	>75 % visų Sandorių atliekama su Lustinių kortelių nuskaitymo aparatais[1] IR >75 % Prekybininko prekybos vietų naudoja kitokią Rizikos mažinimo technologiją[2]

[1] Remiantis „American Express“ vidiniu tyrimu

[2] Remiantis PFI tyrimu

- Padidinta nuolaida (75–100 %) nustatoma pagal mažesniąją Sandorių, atliktų su Lustinių kortelių nuskaitymo aparatais, IR Prekybininkų prekybos vietų, kuriose naudojama kitokia Rizikos mažinimo technologija, procentinę dalį. Pavyzdžiai, pateikti A-6 lentelė: „Padidinta žalos atlyginimo prievolės nuolaida“, parodo, kaip apskaičiuoti žalos atlyginimo nuolaidą.

- Kad jūsų naudojama technologija būtų laikoma Rizikos mažinimo technologija, turite parodyti, kad ji efektyviai naudojama pagal jos sumanymą ir paskirtį.
- Vietų, kuriose naudojama Rizikos mažinimo technologija, procentinė dalis nustatoma atliekant PFI tyrimą.
- Žalos atlyginimo prievolės nuolaida netaikoma jokiems už Duomenų saugumo pažeidimą mokėtiniems mokesčiams.

A-6 lentelė: Padidinta žalos atlyginimo prievolės nuolaida

Pvz.	Naudojama Rizikos mažinimo technologija	Atitinka reikalavimus	Nuolaida
1	• 80 % visų Sandorių atliekama su Lustinių kortelių nuskaitymo aparatais • 0 % prekybos vietų naudoja kitą Rizikos mažinimo technologiją	Ne	50 % – standartinė nuolaida (Rizikos mažinimo technologijos naudojamos mažiau kaip 75 % prekybos vietų nesuteikia teisės į padidintą nuolaidą)[1]
2	• 80 % visų Sandorių atliekama su Lustinių kortelių nuskaitymo aparatais • 77 % prekybos vietų naudoja kitą Rizikos mažinimo technologiją	Taip	77 % – padidinta nuolaida (paremta tuo, kad Rizikos mažinimo technologija naudojama 77 % prekybos vietų)
3	• 93 % visų Sandorių atliekama su Lustinių kortelių nuskaitymo aparatais • 100 % prekybos vietų naudoja kitą Rizikos mažinimo technologiją	Taip	93 % – padidinta nuolaida (paremta tuo, kad 93 % visų Sandorių atliekama su Lustinių kortelių nuskaitymo aparatais)
4	• 40 % visų Sandorių atliekama su Lustinių kortelių nuskaitymo aparatais • 90 % prekybos vietų naudoja kitą Rizikos mažinimo technologiją	Ne	50 % – standartinė nuolaida (mažiau nei 75 % Sandorių, atliktų su Lustinių kortelių nuskaitymo aparatais, nesuteikia teisės į padidintą nuolaidą)

[1] Jeigu Duomenų saugumo pažeidimo metu buvo pažeistas 10 000 „American Express“ kortelių sąskaitų saugumas, mokant po 5 JAV dol. už kiekvieną sąskaitą (10 000 x 5 JAV dol. = 50 000 JAV dol.), gali būti taikoma 50 % nuolaida; tokiu būdu žalos atlyginimo prievolė sumažėja nuo 50 000 iki 25 000 JAV dol. (neįskaitant mokesčių už Duomenų saugumo pažeidimą).

Skirsnis 5 Tikslinės analizės programa (angl. „Targeted Analysis Programme“, TAP)

Kortelės turėtojo duomenų apsaugos pažeidimai gali atsirasti dėl duomenų apsaugos spragų jūsų Kortelės turėtojo duomenų aplinkoje (angl. „Cardholder Data Environment“, CDE).

Kortelės turėtojo duomenų apsaugos pažeidimo pavyzdžiai apima (bet jais neapsiribojama) šiuos:

- **Bendroji pirkimo vieta (angl. „Common Point of Purchase“, CPP):** „American Express“ Kortelės naudotojai praneša apie apgaulingus Sandorius jų Kortelių sąskaitose ir nustatoma, kad jie buvo vykdomi atliekant pirkimus jūsų Įmonėse.
- **Rasti Kortelės duomenys:** „American Express“ Kortelės ir Kortelės turėtojo duomenys rasti žiniatinklyje, susietame su Sandoriais jūsų Įmonėse.
- **Įtariama kenkėjiška programa:** „American Express“ įtaria, kad naudojate programinę įrangą, kuri yra užkrėsta arba kurią gali pažeisti kenkėjiškas kodas.

TAP skirta nustatyti galimus Kortelės turėtojo duomenų apsaugos pažeidimus.

Iš „American Express“ gavę pranešimą apie galimą Kortelės turėtojo duomenų apsaugos pažeidimą, privalote laikytis toliau pateiktų reikalavimų ir privalote įpareigoti jų laikytis Apsaugotąsias šalis.

- Turite nedelsiant peržiūrėti savo CDE dėl duomenų saugumo spragų ir pašalinti visas jų priežastis.
  - Jūsų trečiosios šalies pardavėjas (-ai) privalo atlikti išsamų jūsų CDE tyrimą, jei paslaugos yra užsakomos.
- Gavę „American Express“ pranešimą, turite pateikti peržiūros, vertinimo ir (arba) taisomųjų veiksmų, kurių ėmėtės arba kuriuos suplanavote, santrauką.
- Turite pateikti atnaujintus PCI DSS patvirtinimo dokumentus, vadovaudamiesi Skirsnis 2, „PCI DSS atitikties programa (svarbus periodinis jūsų sistemų atitikties patvirtinimas)“.
- Jei reikia, turite pasitelkti kvalifikuotą PCI PFI, kad jis ištirtų jūsų CDE, jei jūs arba jūsų Apsaugotoji šalis:
  - negalite išspręsti Kortelės turėtojo duomenų apsaugos pažeidimo problemos per pagrįstą „American Express“ nustatytą laikotarpį, arba
  - patvirtinate, kad įvyko Duomenų saugumo pažeidimas, ir laikotės reikalavimų, nustatytų Skirsnis 3, „Duomenų saugumo pažeidimų valdymo įsipareigojimai“.

A-7 lentelė: Mokestis už TAP atitikties neužtikrinimą

Aprašas	1 lygio Prekybininkas arba 1 lygio Paslaugų teikėjas	2 lygio Prekybininkas arba 2 lygio Paslaugų teikėjas	3 lygio arba 4 lygio Prekybininkas
Mokestis už atitikties neužtikrinimą gali būti apskaičiuotas, kai iki pirmo termino neįvykdytos TAP prievolės.	25 000 JAV dol.	5 000 JAV dol.	1 000 JAV dol.
Mokestis už atitikties neužtikrinimą gali būti apskaičiuotas, kai iki antro termino neįvykdytos TAP prievolės.	35 000 JAV dol.	10 000 JAV dol.	2 500 JAV dol.
Mokestis už atitikties neužtikrinimą gali būti apskaičiuotas, kai iki trečio termino neįvykdytos TAP prievolės. **PASTABA.** *Atitikties neužtikrinimo mokesčiai gali būti toliau taikomi tol, kol įvykdomi įsipareigojimai arba išsprendžiama TAP atitikties problema.*	45 000 JAV dol.	15 000 JAV dol.	5 000 JAV dol.

Jei jūsų TAP įsipareigojimai neįvykdomi, „American Express“ turi teisę taikyti sukauptus mokesčius už Atitikties neužtikrinimą, sulaikyti mokėjimus ir (arba) nutraukti Sutartį.

Skirsnis 6 Konfidencialumas

„American Express“ imasi pagrįstų priemonių, kad bendrovė ir jos atstovai bei subrangovai, įskaitant Portalo paslaugų teikėją, užtikrintų jūsų atitikties ataskaitų, įskaitant Patvirtinimo dokumentus, konfidencialumą ir kad neatskleistų Patvirtinimo dokumentų turinio jokioms trečiosioms šalims (išskyrus „American Express“ Susijusias įmones, įgaliotinius, atstovus, Paslaugų teikėjus ir subrangovus) 3 metus nuo jų gavimo datos, išskyrus atvejus, kai šis konfidencialumo įsipareigojimas Patvirtinimo dokumentų turiniui netaikomas, nes:

a. jis buvo žinomas „American Express“ prieš jo atskleidimą;

b. jis tapo viešai prieinamas dėl šio punkto nuostatų pažeidimo, už kurį „American Express“ neatsako;

c. „American Express“ jį teisėtai gavo iš trečiosios šalies, kuri nereikalavo užtikrinti jo konfidencialumo;

d. „American Express“ šį turinį generavo savarankiškai; arba

e. jį būtina atskleisti teismo, administracinės institucijos ar valdžios institucijos reikalavimu arba pagal teisės aktus, taisykles, reglamentus, dėl šaukimo į teismą ar reikalavimo teismui atskleisti informaciją, arba dėl kitokio administracinio ar teisinio proceso, arba gavus kitokią formalią ar neformalią valdžios institucijos ar administracijos (įskaitant priežiūros įstaigas, inspekcijas, tikrintojus ar teisėtvarkos institucijas) užklausą ar reikalavimą.

Skirsnis 7 Atsakomybės atsisakymas

„AMERICAN EXPRESS“ ATSISAKO BET KOKIŲ TIESIOGINIŲ AR NUMANOMŲ, NUMATYTŲ ĮSTATYMAIS ARBA NE PAREIŠKIMŲ, PATVIRTINIMŲ IR ĮSIPAREIGOJIMŲ, SUSIJUSIŲ SU ŠIA DUOMENŲ APSAUGOS UŽTIKRINIMO POLITIKA, PCI DSS, EMV SPECIFIKACIJOMIS, TAIP PAT SU QSA, ASV AR PFI (AR BET KOKIO JŲ DERINIO) PASKYRIMU IR ATLIKIMU, ĮSKAITANT VISUS TINKAMUMO PREKYBAI ARBA TINKAMUMO KONKREČIAI PASKIRČIAI PATVIRTINIMUS. PAGAL ŠIĄ POLITIKĄ „AMERICAN EXPRESS“ KORTELIŲ IŠDAVĖJAI NĖRA TREČIŲJŲ ŠALIŲ NAUDOS GAVĖJAI.

Skirsnis 8 Žodynėlis

Tik šios Duomenų apsaugos užtikrinimo politikos tikslais, taikomi tik šie apibrėžimai:

1 lygio Paslaugų teikėjas – Paslaugų teikėjas su 2,5 mln. ar daugiau „American Express“ kortelių Sandorių per metus; arba bet kuris Paslaugų teikėjas, kurį „American Express“ savo nuožiūra priskiria 1 lygiui.

2 lygio Paslaugų teikėjas – Paslaugų teikėjas su mažiau kaip 2,5 mln. „American Express“ kortelių Sandorių per metus arba bet kuris Paslaugų teikėjas, kurio „American Express“ nepriskyrė 1 lygiui.

1 lygio Prekybininkas – Prekybininkas su 2,5 mln. ar daugiau „American Express“ kortelių Sandorių per metus; arba bet kuris Prekybininkas, kurį „American Express“ dėl kitų priežasčių priskiria 1 lygiui.

2 lygio Prekybininkas – Prekybininkas su nuo 50 000 iki mažiau kaip 2,5 mln. „American Express“ kortelių Sandorių per metus.

3 lygio Prekybininkas – Prekybininkas su nuo 10 000 iki mažiau kaip 50 000 „American Express“ kortelių Sandorių per metus.

4 lygio Prekybininkas – Prekybininkas su mažiau nei 10 000 „American Express“ kortelių Sandorių per metus.

„American Express“ kortelė arba **Kortelė** – bet kokia išdavėjo išduota kortelė, prieigos prie sąskaitos įtaisas arba mokėjimo įtaisas ar paslauga, pažymėta „American Express“ ar jos susijusios įmonės pavadinimu, logotipu, prekės ženklu, paslaugos ženklu, prekės pavadinimu arba kitu firminiu ženklu ar pavadinimu, arba kortelės sąskaitos numeris.

Aprobuota pagal PCI – reiškia, kad įrengti PIN įvedimo aparatai ar Mokėjimo priemonės (arba abu) yra įtraukti į „PCI Security Standards Council, LLC“ aprobuotų įmonių ir teikėjų sąrašą, kuris skelbiamas adresu www.pcisecuritystandards.org.

Aprobuota saugumo patikros įmonė (ASV) – Ūkio subjektas kurį „Payment Card Industry Security Standards Council, LLC“ aprobavo kaip galintį tikrinti, ar laikomasi konkrečių PCI DSS reikalavimų, atliekant prie interneto jungiamų terpių silpnų vietų patikrą.

Aprobuotas Tiesioginio šifravimo (P2PE) sprendimas, įtrauktas į PCI SSC aprobuotų sprendimų sąrašą arba aprobuotas PCI SSC kvalifikuotos saugumo vertinimo P2PE įmonės.

Apsaugos technologijų tobulinimo programa (STEP) – „American Express“ programa, kurioje dalyvaujantys Prekybininkai skatinami diegti didesnį duomenų saugumą užtikrinančias technologijas.

Apsaugotosios šalys – bet kurie arba visi jūsų darbuotojai, įgaliotiniai, atstovai, subrangovai, Duomenų tvarkytojai, Paslaugų teikėjai, jūsų prekybos vietų įrangos (POS) ar sistemų ir mokėjimo duomenų tvarkymo sprendimų teikėjai, Ūkio subjektai, susiję su jūsų „American Express“ Prekybininko sąskaita, ir bet kuri kita šalis, kuriai pagal šią Sutartį gali būti suteikta prieiga prie Kortelės naudotojo duomenų ar Neskelbtinų tapatybės nustatymo duomenų (arba abiejų).

Atitikties patvirtinimas (AOC) – pareiškimas, kad jūsų statusas atitinka PCI DSS, pateikiamas „Payment Card Industry Security Standards Council, LLC“ nustatyta forma.

Atpažinimo ženklas – tai kriptografinis atpažinimo ženklas, pakeičiantis PAN pagal tam tikrą nenuspėjamos vertės indeksą.

Duomenų saugumo pažeidimas – incidentas, kurio metu iš tikrųjų arba tariamai buvo pažeisti „American Express“ šifravimo raktai arba bent vienas „American Express“ kortelės sąskaitos numeris, įskaitant:

- Šifravimo raktų, Kortelės turėtojo duomenų arba Neskelbtinų tapatybės nustatymo duomenų (arba bet kokio šių duomenų derinio), kurie yra laikomi, tvarkomi ar perduodami jums priklausančioje arba jūsų nurodymu naudojamoje, pateikiamoje arba leidžiamoje pasiekti įrangoje, sistemose ir (arba) tinkluose (arba jų komponentuose), neleistiną prieigą ar naudojimą;
- tokių Šifravimo raktų, Kortelės turėtojo duomenų arba Neskelbtinų tapatybės nustatymo duomenų (arba bet kokio šių duomenų derinio) naudojimą nesilaikant šios Sutarties sąlygų ir; arba
- įtariamą arba patvirtintą bet kokių laikmenų, medžiagų, įrašų ar kitokios informacijos su tokiais Šifravimo raktais, Kortelės turėtojo duomenimis arba Neskelbtinais tapatybės nustatymo duomenimis (arba bet kokiu šių duomenų deriniu) praradimą, vagystę arba neteisėtą pasisavinimą bet kokiu būdu.

Duomenų saugumo pažeidimo laikotarpis – įsilaužimo laikotarpis (arba panašiai nustatytas laikotarpis), nurodytas galutinėje teismo ekspertizės ataskaitoje (pvz., PFI ataskaitoje), arba, jei nežinoma, iki 365 dienų iki paskutinio Pranešimo datos apie galimai pažeistus Kortelių numerius, susijusius su mums praneštu Duomenų saugumo pažeidimu.

Duomenų tvarkytojas – Sandorių leidimo ir jų duomenų pateikimo „American Express“ tinklui paslaugų teikėjas Prekybininkams.

EMV sandoris – Sandoris integrinio grandyno kortele (dar vadinama „IC kortele“, „lustine kortele“ „išmaniąja kortele“, „EMV kortele“ arba „ICC“), atliktas naudojantis pardavimo vietos (POS) terminalu, kuriuo galima nuskaityti IC korteles ir kuris turi galiojantį ir nepasenusį EMV tipo patvirtinimą. Su EMV tipo patvirtinimais galima susipažinti interneto svetainėje www.emvco.com.

EMV specifikacijos – įmonės „EMVCo, LLC“ parengtos specifikacijos, skelbiamos adresu www.emvco.com.

Franšizės davėjas – verslo valdytojas, suteikiantis fiziniams ar juridiniams asmenims (Franšizės gavėjams) licenciją platinti prekes ir (arba) paslaugas pagal licenciją arba vykdyti veiklą su valdytojo Prekės ženklu; teikia pagalbą Franšizės gavėjams vykdant veiklą arba turi įtakos Franšizės gavėjų veiklos būdui bei ima iš Franšizės gavėjų mokestį.

Franšizės gavėjas – nepriklausoma nuosavybės ir valdymo atžvilgiu trečioji šalis (įskaitant franšizės gavėją, licencijos savininką arba skyrių), išskyrus Susijusią įmonę, kuriai Franšizės davėjas suteikė licenciją valdyti franšizę ir kuri yra sudariusi rašytinę sutartį su Franšizės davėju, pagal kurią ji nuolat naudoja išorinio atpažinimo elementus, aiškiai save identifikuodama su Franšizės davėjo Prekės ženklais, arba viešai prisistato kaip Franšizės davėjo įmonių grupės narė.

Įsivertinimo anketa (SAQ) – „Payment Card Industry Security Standards Council, LLC“ sukurta savarankiško vertinimo priemonė, skirta PCI DSS atitikčiai vertinti ir patvirtinti.

Kortelės išdavėjas – bet kuris Ūkio subjektas (įskaitant „American Express“ ir jos Susijusias įmones), kuriam „American Express“ arba „American Express“ Susijusi įmonė suteikė licenciją išduoti Korteles ir vykdyti Kortelių išdavimo veiklą.

Kortelės naudotojas – individualus asmuo arba ūkio subjektas, (i) kuris yra sudaręs sutartį su išdavėju dėl Kortelės sąskaitos atidarymo arba (ii) kurio pavadinimas / vardas ir pavardė nurodyti ant Kortelės.

Kortelės naudotojo informacija – informacija apie „American Express“ Kortelės naudotojus ir Kortelių sandorius, įskaitant pavadinimus, vardus ir pavardes, adresus, kortelių sąskaitų numerius ir kortelių identifikavimo numerius (angl. „Card Identification“, CID).

Kortelės numeris – unikalus identifikavimo numeris, kurį Išdavėjas priskiria išduodamai Kortelei.

Kortelės turėtojas – tai klientas, kuriam išduota mokėjimo kortelė, arba bet koks asmuo, įgaliotas naudotis mokėjimo kortele

Kortelės turėtojo duomenys – tai mažiausiai visas Pirminis sąskaitos numeris (PAN) arba visas PAN ir bet kurie šie duomenys: kortelės turėtojo vardas, pavardė, galiojimo laikas ir (arba) paslaugos kodas. Apie papildomus duomenų elementus, kurie gali būti perduodami arba tvarkomi (bet ne saugomi) kaip mokėjimo sandorio dalis, žr. Neskelbtinus tapatybės nustatymo duomenis.

Kortelės turėtojo duomenų aplinka (CDE) – žmonės, procesai ir technologijos, kurie saugo, apdoroja arba perduoda kortelės turėtojo duomenis arba neskelbtinus tapatybės nustatymo duomenis.

Kreditas – Mokesčio suma, kurią grąžinate Kortelės naudotojui už su Kortele įsigytus pirkinius arba atliktus mokėjimus.

Kredito įrašas – tai Kredito įrašas, atitinkantis mūsų reikalavimus.

Kvalifikuotas saugumo vertintojas (QSA) – ūkio subjektas, „Payment Card Industry Security Standards Council, LLC“ aprobuotas kaip galintis tikrinti, ar laikomasi PCI DSS reikalavimų.

Lustas – Kortelėje integruota mikroschema su Kortelės naudotojo ir sąskaitos informacija.

Lustinė kortelė – Kortelė su Lustu, kurią naudojant ir norint patikrinti Kortelės naudotojo tapatybę arba Luste esančią sąskaitos informaciją (arba abu šiuos dalykus) gali reikėti įvesti PIN kodą (mūsų medžiagoje dar gali būti vadinama „išmaniąja kortele“, „EMV kortele“, „ICC“ arba „integrinio grandyno kortele“).

Lustinių kortelių nuskaitymo aparatas – pardavimo vietoje naudojamas aparatas su galiojančiu ir nepasenusiu EMVCo (www.emvco.com) sertifikatu, kuriuo galima atlikti AEIPS atitinkančius Lustinių kortelių Sandorius.

Mokėjimo kortelių pramonės apsaugos standartų tarybos (PCI SSC) reikalavimai – standartų ir reikalavimų, susijusių su mokėjimo kortelių duomenų apsauga ir sauga, įskaitant PCI DSS ir PA DSS, rinkinys, kuris skelbiamas adresu www.pcisecuritystandards.org.

Mokėjimo kortelių pramonės duomenų apsaugos standartas (PCI DSS) – Mokėjimo kortelių pramonės duomenų apsaugos standartas, skelbiamas adresu www.pcisecuritystandards.org.

Mokėjimo įrašas – tai atkuriamas (popierinis ir elektroninis) Mokėjimo įrašas, atitinkantis mūsų reikalavimus, kuriame nurodomas Kortelės numeris, Sandorio data, suma doleriais, Patvirtinimas, Kortelės naudotojo parašas (jei taikoma) ir kita informacija

Mokėjimo priemonė – terminas vartojamas reikšme, apibrėžta Saugios programinės įrangos standarto ir Saugios programinės įrangos gyvavimo ciklo standarto terminų žodyne, kuris skelbiamas adresu www.pcisecuritystandards.org.

Mokestis – mokėjimas arba pirkimas, atliktas Kortele.

Neskelbtini tapatybės nustatymo duomenys – tai su saugumu susijusi informacija, naudojama kortelių turėtojams autentifikuoti ir (arba) mokėjimo kortelių sandoriams autorizuoti. Ši informacija apima, be kita ko, kortelės tikrinimo kodus, išsamius sekimo duomenis (iš magnetinės juostelės arba lygiaverčio lusto), PIN kodus ir PIN blokatorius.

Pardavimo vieta (POS) – informacijos apdorojimo sistema arba įranga, įskaitant terminalą, asmeninį kompiuterį, elektroninį kasos aparatą, bekontaktį skaitytuvą arba mokėjimų apdorojimo variklį arba procesą, kurį Prekybininkas naudoja gauti tapatybės patvirtinimus arba surinkti Sandorio duomenis, arba abu šiuos dalykus.

Paslaugų teikėjai – įgaliotieji duomenų tvarkytojai, trečiųjų šalių duomenų tvarkytojai, prieigos teikėjai, POS sistemų integruotojai ir kiti asmenys, teikiantys Prekybininkams POS sistemų paslaugas ar kitokius mokėjimo apdorojimo sprendimus ar paslaugas.

Patvirtinimo dokumentai – AOC, atliktas ryšium su Metiniu objekto saugumo vertinimu, arba SAQ, AOSC ir išvadų suvestinės, parengtos ryšium su Ketvirtinėmis tinklo saugumo patikromis, arba Metinė atestacija pagal Apsaugos technologijų tobulinimo programą.

Pažeistas kortelės numeris – „American Express“ kortelės sąskaitos numeris, susijęs su Duomenų saugumo pažeidimu.

PCI DSS – Mokėjimo kortelių pramonės duomenų apsaugos standartas, skelbiamas adresu www.pcisecuritystandards.org.

PCI PIN saugumo reikalavimai – Mokėjimo kortelių pramonės PIN saugumo reikalavimai, skelbiami adresu www.pcisecuritystandards.org.

PCI teisminės ekspertizės specialistas (PFI) – ūkio subjektas, „Payment Card Industry Security Standards Council, LLC“ atestuotas atlikti teisminės ekspertizės tyrimus, kai pažeidžiamas mokėjimo Kortelių duomenų saugumas.

PIN įvedimo aparatas – terminas vartojamas reikšme, apibrėžta Mokėjimo kortelių pramonės PIN Sandorių apsaugos (PIN Transaction Security, PTS) sąveikos vietos (Point of Interaction, POI) modulinio saugumo reikalavimų terminų žodyne, kuris skelbiamas adresu www.pcisecuritystandards.org.

Pirkėjo inicijuoto mokėjimo (BIP) Sandoris – elektroninis mokėjimo sprendimas, leidžiantis pirkėjams greitai ir veiksmingai planuoti mokėjimus tiekėjams (susietas su įmonės kortelėmis).

Pirminis sąskaitos numeris (PAN) – terminas vartojamas galiojančiame PCI DSS terminų žodyne apibrėžta reikšme.

Portalas – ataskaitų teikimo sistema, kurią parūpina „American Express“ pasirinktas „American Express“ PCI programos administratorius. Prekybininkai ir Paslaugų teikėjai privalo naudoti Portalą PCI patvirtinimo dokumentams teikti „American Express“.

Pranešimo data – data, kai „American Express“ pateikia išdavėjams galutinį pranešimą apie Duomenų saugumo pažeidimą. Ši data priklauso nuo to, kada „American Express“ gavo galutinę ekspertizės ataskaitą arba vidinio tyrimo ataskaitą; ją savo nuožiūra nustato „American Express“.

Prekybininkas – Prekybininkas ir visos jo susijusios įmonės, pagal Sutartį su „American Express“ arba su jos susijusiomis įmonėmis priimančios „American Express“ korteles.

Prekybininko lygis – tai Prekybininkams skiriamas pavadinimas, susijęs su jų PCI DSS atitikties patvirtinimo įsipareigojimais, kaip aprašyta Skirsnis 2, „PCI DSS atitikties programa (svarbus periodinis jūsų sistemų atitikties patvirtinimas)“.

Programa – tai „American Express“ PCI atitikties programa.

Rizikos mažinimo technologija – technologinis sprendimas, „American Express“ nuožiūra užtikrinantis geresnę „American Express“ Kortelės turėtojo duomenų ir Neskelbtinų tapatybės nustatymo duomenų apsaugą. Kad jūsų naudojama technologija būtų laikoma Rizikos mažinimo technologija, turite parodyti, kad ji efektyviai naudojama pagal jos sumanymą ir paskirtį. Keli pavyzdžiai, bet jais neapsiribojama: EMV, Tiesioginis šifravimas ir pakaitos simboliai.

Sandoris – tai Kortele atlikta Mokėjimo, Kredito, Grynųjų pinigų išdavimo (arba kitokio grynųjų pinigų gavimo) arba Bankomato operacija.

Sandorio duomenys – tai visa „American Express“ reikalaujama informacija, patvirtinanti vieną ar daugiau Sandorių, įskaitant informaciją, gautą pardavimo vietoje, informaciją, gautą ar sukurtą Tapatybės patvirtinimo ir Pateikimo metu, ir bet kokį Mokėjimo atšaukimą.

Sąskaitos duomenis – sudaro Kortelės turėtojo duomenys ir (arba) neskelbtini tapatybės nustatymo duomenys. Žr. Kortelės turėtojo duomenys ir Neskelbtini tapatybės nustatymo duomenys.

Saugumo atitikties patvirtinimas (AOSC) – tinklo saugumo patikra pagrįstas pareiškimas, kad jūsų statusas atitinka PCI DSS, pateikiamas „Payment Card Industry Security Standards Council, LLC“ nustatyta forma.

Šifravimo raktas („American Express“ šifravimo raktas) – visi raktai, naudojami tvarkant, generuojant, įkeliant ir (arba) apsaugant sąskaitos duomenis. Prie Šifravimo raktų, be kita ko, priskiriami toliau nurodyti raktai:

- Pagrindiniai šifravimo raktai: zoninis pagrindinis raktas (angl. „Zone Master Key“, ZMK) ir zoninis PIN raktas (angl. „Zone Pin Key“, ZPK)
- Pagrindiniai raktai, naudojami saugiuose kriptografijos aparatuose: vietinis pagrindinis raktas (angl. „Local Master Key“, LMK)
- Kortelių apsaugos kodų raktas (angl. „Card Security Code Key“, CSCK)
- PIN raktai: bazinis išvestinis raktas (angl. „Base Derivation Key“, BDK), PIN šifravimo raktas (angl. „PIN Encryption Key“, PEK) ir ZPK

Sutartis – tai Bendrosios nuostatos, Prekybininkų taisyklės ir visi pridėti priedai ir papildymai (kartais mūsų medžiagoje vadinama Kortelės priėmimo sutartis).

Tiesioginis šifravimas (P2PE) – sprendimas, kriptografiškai saugantis sąskaitos duomenis, juos perduodant iš tos vietos, kurioje Prekybininkas priima mokėjimo kortelę, į saugią iššifravimo vietą.

Tikslinės analizės programa – programa, leidžianti anksti nustatyti galimą Kortelės turėtojo duomenų apsaugos pažeidimą jūsų Kortelės turėtojo duomenų aplinkoje (CDE). Žr. Skirsnis 5, „Tikslinės analizės programa (angl. „Targeted Analysis Programme“, TAP)“.

Teisminės ekspertizės incidento galutinės ataskaitos šablonas – tai šablonas, kurį galima gauti iš „PCI Security Standards Council“, interneto svetainėje www.pcisecuritystandards.org.

Vartotojas – tai kortelės turėtojas, perkantis prekes, paslaugas arba ir viena, ir kita.

Skirsnis 9 Naudingos svetainės

„American Express“ duomenų saugumas: www.americanexpress.com/datasecurity

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

EMVCo: www.emvco.com