

# Prevádzkové zásady týkajúce sa bezpečnosti údajov (DSOP)

|                 |                                                                                                               |           |
|-----------------|---------------------------------------------------------------------------------------------------------------|-----------|
| <b>Oddiel 1</b> | <b>Úvodné informácie o zásadách DSOP a Normách Ochrany</b> . . . . .                                          | <b>3</b>  |
| <b>Oddiel 2</b> | <b>Program dodržiavania predpisov PCI DSS (dôležité periodické overovanie vašich systémov)</b> . . . . .      | <b>3</b>  |
| Krok 1:         | Účasť na Programe dodržiavania predpisov spoločnosti American Express v súlade s týmito Zásadami . . . . .    | 4         |
| Krok 2:         | Oboznámenie sa s Úrovňou Obchodníka/Poskytovateľa služieb a Požiadavkami na Overovaciu Dokumentáciu . . . . . | 4         |
| Krok 3:         | Vyplnenie Overovacej dokumentácie, ktorú musíte poslať spoločnosti American Express . . . . .                 | 7         |
| Krok 4:         | Poslanie Overovacej dokumentácie spoločnosti American Express . . . . .                                       | 9         |
| <b>Oddiel 3</b> | <b>Povinnosť spravovať Incidenty týkajúce sa údajov</b> . . . . .                                             | <b>10</b> |
| <b>Oddiel 4</b> | <b>Povinnosti súvisiace s Odškodnením za Incident týkajúci sa údajov</b> . . . . .                            | <b>12</b> |
| <b>Oddiel 5</b> | <b>Program cielenej analýzy (TAP)</b> . . . . .                                                               | <b>14</b> |
| <b>Oddiel 6</b> | <b>Dôvernosť</b> . . . . .                                                                                    | <b>15</b> |
| <b>Oddiel 7</b> | <b>Vyhlásenie o odmietnutí zodpovednosti</b> . . . . .                                                        | <b>16</b> |
| <b>Oddiel 8</b> | <b>Glosár</b> . . . . .                                                                                       | <b>16</b> |
| <b>Oddiel 9</b> | <b>Užitočné webové stránky</b> . . . . .                                                                      | <b>20</b> |

# Súhrn zmien zásad DSOP

## Ikony

Dôležité aktualizácie sú uvedené v Tabuľke súhrnu zmien a zároveň sú v dokumente *DSOP* označené pruhom. Pruhy na označenie zmien sú zvislé čiary zvyčajne na ľavom okraji a označujú pridaný alebo upravený text. Pruhom na označenie zmien, ktorý je znázornený na ľavom okraji, sú označené len podstatné zmeny v dokumente *DSOP* s potenciálnymi vplyvmi na prevádzkové postupy Obchodníka.



Odstránený text je zvýraznený ikonou odpadkového koša umiestnenou na okraji vedľa každého významného odstránenia textu vrátane oddielov, tabuliek, odsekov, poznámok a odrážok. Pri odkazovaní na odstránený text sa v tomto Súhrne zmien používa číslovanie oddielov z predchádzajúcej publikácie, aby sa predišlo nejasnostiam.

---

Modré čiary ohraničujúce odseky označujú informácie pre konkrétny región.

---

## Tabuľka súhrnu zmien

Dôležité aktualizácie sú uvedené v nasledujúcej tabuľke a zároveň sú v dokumente *DSOP* označené pruhom.

| Oddiel/Pododdiel                      | Opis zmeny |
|---------------------------------------|------------|
| Pre toto vydanie nie sú žiadne zmeny. |            |

## Oddiel 1

## Úvodné informácie o zásadách DSOP a Normách Ochrany

**Spoločnosť American Express má ako líder v oblasti ochrany spotrebiteľov dlhodobý záväzok chrániť Údaje o držiteľoch kariet a Citlivé overovacie údaje a zaisťovať, že sa bezpečne uchovávajú.**

Ohrozené údaje majú negatívny vplyv na spotrebiteľov, Obchodníkov, Poskytovateľov služieb a vydavateľov kariet. Aj jediný incident môže vážne poškodiť povesť spoločnosti a znemožniť jej efektívne obchodovať. Dôveru zákazníkov, ziskovosť a povesť spoločnosti môže pomôcť podporiť to, že spoločnosť sa tejto hrozbe venuje a vytvára si bezpečnostné prevádzkové zásady.

V spoločnosti American Express vieme, že naši Obchodníci a Poskytovatelia služieb (spoločne uvádzané ako vy) sa takisto zaoberajú touto témou, a v rámci vašich záväzkov od **vás** vyžadujeme, aby ste dodržiavali ustanovenia týkajúce sa bezpečnosti údajov uvedené vo vašej dohode o prijímaní (v prípade Obchodníkov) alebo spracovaní (v prípade Poskytovateľov služieb) Karty American Express® (v oboch prípadoch uvádzané ako **Dohoda**) a tieto Prevádzkové zásady týkajúce sa bezpečnosti údajov (DSOP), ktoré môžeme z času na čas meniť. Tieto požiadavky sa vzťahujú na všetky vaše zariadenia, systémy a siete (a ich súčasti), v ktorých sa ukladajú, spracúvajú alebo prenášajú Šifrovacie kľúče, Údaje o držiteľoch kariet alebo Citlivé overovacie údaje (alebo ich kombinácia).

*Význam pojmov uvedených s veľkým začiatočným písmenom, ktoré nie sú vysvetlené v tomto dokumente, je vymedzený v glosári na konci týchto zásad.*

Prevádzkové zásady týkajúce sa bezpečnosti údajov (DSOP) sú súborom komplexných požiadaviek určených na ochranu Údajov o účtoch vždy, keď sa tieto údaje uchovávajú, spracúvajú alebo prenášajú.

Spoločnosť American Express vyžaduje od všetkých Obchodníkov a Poskytovateľov služieb, aby dodržiavali Normu týkajúcu sa bezpečnosti údajov pre odvetvie platobných kariet (PCI DSS). V rámci tejto požiadavky musíte dodržiavať nasledujúce predpisy a zabezpečiť, že ich budú dodržiavať aj všetky Strany, ktoré zastupujete. Konkrétne musíte:

- ukladať Údaje o držiteľoch kariet len na účely realizácie Transakcií kartami American Express v súlade s Dohodou a s jej požiadavkami,
- dodržiavať platnú verziu PCI DSS (Norma týkajúca sa bezpečnosti údajov pre odvetvie platobných kariet) a iných Požiadaviek Rady pre PCI Security Standards Council (PCI-SSC), ktoré sa vzťahujú na spracovanie, ukladanie alebo prenášanie Šifrovacích kľúčov, Údajov o držiteľoch kariet alebo Citlivých overovacích údajov najneskôr odo dňa nadobudnutia účinnosti príslušnej Požiadavky,
- zaisťiť použitie produktov schválených pre oblasť PCI pri nasadzovaní alebo výmene technológie na uchovávanie, spracovanie alebo prenos údajov.

Musíte chrániť všetky záznamy o Platbách kartami American Express a záznamy o Refundáciách na tieto karty uchovávané podľa Dohody v súlade s týmito ustanoveniami o bezpečnosti údajov, používať tieto záznamy len na účely stanovené v Dohode a náležite ich zabezpečiť. Voči spoločnosti American Express máte finančnú aj inú zodpovednosť za to, že Strany, ktoré zastupujete, budú dodržiavať tieto ustanovenia o bezpečnosti údajov (okrem toho, že ste zodpovední za preukázanie, že Strany, ktoré zastupujete, dodržiavajú tieto pokyny podľa [Oddielu 2, „Program dodržiavania predpisov PCI DSS \(dôležité periodické overovanie vašich systémov\)“](#), s výnimkou prípadov uvedených v danom oddieli). Podrobnosti o normách PCI a o tom, ako dodržiavať ich požiadavky, nájdete na adrese [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

## Oddiel 2

## Program dodržiavania predpisov PCI DSS (dôležité periodické overovanie vašich systémov)

Musíte vykonať nasledujúce kroky, aby ste v rámci PCI DSS ročne a každých 90 dní overili nižšie opísaným spôsobom stav zariadenia, systémov a/alebo sietí vašich a vašich Franchisantov (a ich komponentov), na ktorých sú Údaje o držiteľoch kariet alebo Citlivé overovacie údaje uložené, spracované alebo prenesené.

Overenie pozostáva zo štyroch krokov:

- [Krok 1:](#) Účasť na programe dodržiavania predpisov PCI spoločnosti American Express v súlade s týmito zásadami.
- [Krok 2:](#) Oboznámenie sa s Úrovňou Obchodníka/Poskytovateľa služieb a Požiadavkami na Overovaciu dokumentáciu.
- [Krok 3:](#) Vyplnenie Overovacej dokumentácie, ktorú musíte poslať spoločnosti American Express.
- [Krok 4:](#) Poslanie Overovacej dokumentácie spoločnosti American Express v stanovenom termíne.

## Krok 1: Účasť na Programe dodržiavania predpisov spoločnosti American Express v súlade s týmito Zásadami

Obchodníci 1. úrovne, Obchodníci 2. úrovne a všetci Poskytovatelia služieb, ako je popísané nižšie, sa musia zúčastniť Programu v súlade s týmito zásadami. Spoločnosť American Express môže na základe vlastného uváženia určiť konkrétnych Obchodníkov 3. a 4. úrovne, aby sa zúčastnili v Programe v súlade s týmito zásadami.

Obchodníci a Poskytovatelia služieb, od ktorých sa vyžaduje účasť v Programe, sa musia zaregistrovať na [Portáli](#) poskytovanom Správcom Programu vybraným spoločnosťou American Express v stanovenom termíne.

- Musíte prijať všetky primerané podmienky spojené s používaním Portálu.
- Musíte priradiť a poskytnúť presné informácie aspoň pre jeden kontakt na zabezpečenie údajov v rámci Portálu. Požadované informácie zahŕňajú:
  - celé meno
  - e-mailová adresa
  - telefónne číslo
  - fyzická poštová adresa
- Pri zmene informácií musíte poskytnúť aktualizované alebo nové kontaktné informácie pre priradený kontakt na zabezpečenie údajov v rámci Portálu.
- Musíte sa uistiť, že vaše systémy sú aktualizované, aby umožňovali servisnú komunikáciu z určenej domény Portálu.

Vaše neposkytnutie alebo neudržiavanie aktuálnych kontaktných informácií na zabezpečenie údajov alebo povolenie e-mailovej komunikácie neovplyvní naše práva na vymieranie poplatkov.

## Krok 2: Oboznámenie sa s Úrovňou Obchodníka/Poskytovateľa služieb a Požiadavkami na Overovaciu Dokumentáciu

Obchodníci sa rozdeľujú do štyroch Úrovní Obchodníka a Poskytovateľa služieb do dvoch Úrovní, a to na základe objemu Transakcií kartami American Express.

- Pre Obchodníkov je to objem odoslaný ich Prevádzkami, ktoré dosahujú najvyššiu úroveň účtu Obchodníka American Express.\*
- V prípade Poskytovateľov služieb je to súčet objemov predložených Poskytovateľom služieb a Subjektmi poskytovateľa služieb, ktorým poskytujete služby.

Do objemu Transakcií kartami American Express na určenie úrovne Obchodníka a požiadaviek overenia sa nepočítajú Transakcie súvisiace s Platbami iniciovanými kupujúcimi (BIP). Budete patriť do jednej z Úrovní Obchodníka uvedených v [Tabuľke A-1 Úrovně Obchodníka a Poskytovateľa služieb](#).

\*V prípade Franchisorov to zahŕňa objemy zo Zariadení ich Franchisantov. Franchisori, ktorí poverili svojich Franchisantov, aby používali určený Platobný systém v mieste predaja (POS) alebo Poskytovateľa služieb, musia tiež poskytnúť Overovaciu dokumentáciu týkajúcu sa dotknutých Franchisantov.

Tabuľka A-1: Úrovne Obchodníka a Poskytovateľa služieb

| Úroveň Obchodníka              | Ročné Transakcie American Express                                                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Obchodník 1. úrovne            | 2,5 milióna a viac Transakcií kartami American Express ročne alebo akýkoľvek Obchodník, ktorému spoločnosť American Express na základe vlastného uváženia prideli 1. úroveň.             |
| Obchodník 2. úrovne            | 50 000 až menej ako 2,5 milióna Transakcií kartami American Express ročne.                                                                                                               |
| Obchodník 3. úrovne            | 10 000 až menej ako 50 000 Transakcií kartami American Express ročne.                                                                                                                    |
| Obchodník 4. úrovne            | Menej ako 10 000 Transakcií kartami American Express ročne.                                                                                                                              |
| Úroveň Poskytovateľa služieb   | Ročné Transakcie American Express                                                                                                                                                        |
| Poskytovateľ služieb 1. úrovne | 2,5 milióna a viac Transakcií kartami American Express ročne alebo akýkoľvek Poskytovateľ služieb, ktorého spoločnosť American Express považuje za Poskytovateľa služieb 1. úrovne.      |
| Poskytovateľ služieb 2. úrovne | menej ako 2,5 milióna Transakcií kartami American Express ročne alebo akýkoľvek Poskytovateľ služieb, ktorého spoločnosť American Express nepovažuje za Poskytovateľa služieb 1. úrovne. |

## Požiadavky na Overovaciu dokumentáciu Obchodníka

Obchodníci (nie Poskytovatelia služieb) majú štyri možné klasifikácie Úrovne Obchodníka. Po stanovení úrovne Obchodníka z [Tabuľky A-1 Úrovne Obchodníka a Poskytovateľa služieb](#) (vyššie) si pozrite [Tabuľku A-2 Požiadavky na Overovaciu dokumentáciu Obchodníka](#) a stanovte si požiadavky na Overovaciu dokumentáciu.

**Tabuľka A-2: Požiadavky na Overovaciu dokumentáciu Obchodníka**

| Úroveň Obchodníka/<br>Ročné Transakcie American Express | Správa o zhode<br>Osvedčenie o súlade (ROC AOC) | Samohodnotiaci dotazník<br>Osvedčenie o súlade (SAQ AOC) A Štvrťročná kontrola<br>externej sieťovej zraniteľnosti (Kontrola) | Osvedčenie Program na posilnenie bezpečnostných technológií (STEP) pre Obchodníkov s nárokom na zaradenie do programu |
|---------------------------------------------------------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Úroveň 1/<br>2,5 milióna alebo viac                     | Povinné                                         | Nevzťahuje sa                                                                                                                | Voliteľné so súhlasom American Express (nahrádza ROC)                                                                 |
| Úroveň 2/<br>50 000 až menej ako 2,5 milióna            | Voliteľné                                       | SAQ AOC povinné (ak sa neodošlo ROC AOC); povinná kontrola pri určitých typoch SAQ                                           | Voliteľné so súhlasom American Express* (nahrádza SAQ a kontrolu siete alebo ROC)                                     |
| Úroveň 3**/<br>10 000 až menej ako 50 000               | Voliteľné                                       | SAQ AOC voliteľné (povinné, ak to vyžaduje spoločnosť American Express); povinná kontrola pri určitých typoch SAQ            | Voliteľné so súhlasom American Express* (nahrádza SAQ a kontrolu siete alebo ROC)                                     |
| Úroveň 4**/<br>Menej ako 10 000                         | Voliteľné                                       | SAQ AOC voliteľné (povinné, ak to vyžaduje spoločnosť American Express); povinná kontrola pri určitých typoch SAQ            | Voliteľné so súhlasom American Express* (nahrádza SAQ a kontrolu siete alebo ROC)                                     |

\* **Poznámka:** Tím PCI spoločnosti American Express posúdi žiadosť a oprávnenosť a určí, či máte nárok na zaradenie do Programu STEP. Ak chcete skontrolovať oprávnenosť, kontaktujte svojho klientskeho manažéra a/alebo [AXPPCIComplianceProgram@aexp.com](mailto:AXPPCIComplianceProgram@aexp.com).

\*\*Na účel vylúčenia pochybnosti, Obchodníci 3. a 4. úrovne nemusia odovzdávať Overovaciu dokumentáciu, ak to spoločnosť American Express podľa vlastného uváženia nevyžaduje. Napriek tomu sú však povinní dodržiavať všetky ostatné ustanovenia týchto Prevádzkových zásad týkajúcich sa bezpečnosti údajov a nesú za ich dodržiavanie zodpovednosť.

Spoločnosť American Express si vyhradzuje právo overiť úplnosť, presnosť a vhodnosť vašej Overovacej dokumentácie PCI. Spoločnosť American Express môže vyžadovať, aby ste poskytli ďalšie podporné dokumenty na vyhodnotenie na podporu tohto účelu. Okrem toho má American Express právo požadovať, aby ste zapojili Kvalifikovaného hodnotiteľa bezpečnosti (QSA) alebo Forezného vyšetrovateľa pre oblasť PCI (PFI) schváleného Radou pre PCI Security Standards Council.

## Požiadavky na Overovaciu dokumentáciu Poskytovateľa služieb

Poskytovatelia služieb (nie Obchodníci) majú dve možné klasifikácie Úrovní. Po stanovení úrovne Poskytovateľa služieb z [Tabuľky A-1 Úrovně Obchodníka a Poskytovatele služieb](#) (vyššie) si pozrite [Tabuľku A-3 Overovacia dokumentácia Poskytovateľa služieb](#) a stanovte si požiadavky na Overovaciu dokumentáciu.

Poskytovatelia služieb nemajú nárok na zaradenie do Programu STEP.

**Tabuľka A-3: Overovacia dokumentácia Poskytovateľa služieb**

| Úroveň | Overovacia dokumentácia                                                                                                                          | Požiadavka |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 1      | Výročná správa o zhode Osvedčenie o súlade (ROC AOC)                                                                                             | Povinné    |
| 2      | Výročný SAQ D (Poskytovateľ služieb) a Štvrťročná kontrola siete alebo Výročná správa o zhode Osvedčenie o súlade (ROC AOC), ak sa uprednostňuje | Povinné    |

Odporúča sa, aby Poskytovatelia služieb tiež dodržiavali postupy Dodatočného overenia určených subjektov PCI.

## Program na posilnenie bezpečnostných technológií (STEP)

Obchodníci, ktorí dodržiavajú PCI DSS, môžu mať na základe uváženia spoločnosti American Express nárok na zaradenie do Programu STEP spoločnosti American Express, ak vo svojich prostriedkoch na spracovanie Kariet nasadzujú určité dodatočné bezpečnostné technológie. Program STEP sa vzťahuje len na Obchodníkov, ktorí v priebehu predchádzajúcich 12 mesiacov nemali Incident týkajúci sa Údajov a ktorí uskutočnili aspoň 75 % všetkých Transakcií kartami využitím kombinácie nasledujúcich možností rozšíreného zabezpečenia:

- **EMV, EMV Bezkontaktná alebo Digitálna peňaženka** – v aktívnom Zariadení s podporou čipov, ktoré má platné a aktuálne schválenie/certifikát EMVCo ([www.emvco.com](http://www.emvco.com)) a dokáže spracovávať Transakcie čipovými kartami v súlade s AEIPS. (Obchodníci v USA sú povinní zahrnúť Bezkontaktné transakcie)
- **Šifrovanie Point-to-Point (P2PE)** – sprostredkované Obchodníkovmu spracovateľovi pomocou systému Šifrovania Point-to-Point Schváleného Radou PCI SSC alebo QSA.
- **Tokenizované** – implementované riešenie tokenizácie musí:
  - spĺňať špecifikácie EMVCo,
  - byť zabezpečené, spracované, uložené, prenášané a úplne spravované poskytovateľom služieb tretej strany v súlade s PCI a
  - Token nie je možné vrátiť späť, aby odhalil Obchodníkovi nezamaskované Primárne čísla účtov (PAN).

Na Obchodníkov, ktorí majú nárok na zaradenie do Programu STEP, sa vzťahujú znížené požiadavky na Overovaciu Dokumentáciu PCI, ako sa opisuje v [Kroku 3: „Vyplnenie Overovacej dokumentácie, ktorú musíte poslať spoločnosti American Express“](#) nižšie.

## Krok 3: Vyplnenie Overovacej dokumentácie, ktorú musíte poslať spoločnosti American Express

Nasledujúce dokumenty sa vyžadujú pre rôzne úrovne Obchodníkov a Poskytovateľov služieb, ako uvádza [Tabuľka A-2: Požiadavky na Overovaciu dokumentáciu Obchodníka](#) a [Tabuľka A-3: Overovacia dokumentácia Poskytovateľa služieb](#) vyššie.

Musíte poskytnúť Osvedčenie o súlade (AOC) pre príslušný typ hodnotenia. AOC je vyhlásenie o vašom stave súladu a ako také musí byť podpísané s dátumom príslušnou úrovňou vedenia vo vašej organizácii.

Okrem AOC od vás môže spoločnosť American Express vyžadovať, aby ste poskytli kópiu úplného hodnotenia a podľa nášho uváženia aj ďalšie podporné dokumenty preukazujúce súlad s požiadavkami PCI DSS. Táto Overovacia dokumentácia je vyplnená na vaše náklady.

**Správa o zhode Osvedčenie o súlade (ROC AOC) – (ročná požiadavka)** – Správa o zhode dokumentuje výsledky podrobného preskúmania vašich zariadení, systémov a sietí (a ich komponentov) na mieste, kde sa ukladajú, spracúvajú alebo prenášajú údaje o Držiteľoch kariet alebo Citlivé overovacie údaje (alebo oboje). Existujú dve verzie: jedna pre Obchodníkov a druhá pre Poskytovateľov služieb. Správa o zhode musí byť vykonaná:

- QSA, alebo
- Interným hodnotiteľom bezpečnosti (ISA) a potvrdená vašim výkonným riaditeľom, finančným riaditeľom, riaditeľom informačnej bezpečnosti alebo riaditeľom

Správa ROC AOC musí byť podpísaná a označená dátumom QSA alebo ISA a oprávnenou úrovňou vedenia vo vašej organizácii a musí byť poskytnutá spoločnosti American Express aspoň raz za rok.

**Samohodnotiaci dotazník osvedčenia o súlade (SAQ AOC) – (ročná požiadavka)** – Samohodnotiace dotazníky umožňujú samokontrolu vášho zariadenia, systémov a sietí (a ich komponentov), kde sa ukladajú, spracúvajú alebo prenášajú Údaje o Držiteľoch kariet alebo Citlivé overovacie údaje (alebo oboje). Existuje viacero verzií SAQ. Vyberiete si jeden alebo viac na základe Prostredia údajov o držiteľoch kariet.

SAQ môže vyplniť personál vašej Spoločnosti, ktorý je kvalifikovaný na presné a dôkladné zodpovedanie otázok, alebo môžete na pomoc využiť službu QSA. SAQ AOC musí byť podpísané a označené dátumom oprávnenou úrovňou vedenia vo vašej organizácii a musí byť poskytnuté spoločnosti American Express aspoň raz za rok.

**Zhrnutie kontroly externej sieťovej zraniteľnosti (ASV Scan) schváleným kontrolórom – (90-dňová požiadavka)** – Kontrola externej zraniteľnosti je test na diaľku, ktorý vám pomôže identifikovať potenciálne slabé stránky, zraniteľnosti a nesprávne konfigurácie komponentov vášho Prostredia údajov o držiteľoch kariet (napr. webových stránok, aplikácií, webových serverov, poštových serverov, verejne prístupných domén alebo hostiteľov).

Kontrolu ASV musí vykonať Schválený dodávateľ kontroly (ASV).

Ak to vyžaduje SAQ, Kontrolná správa ASV osvedčenia kontroly súladu (AOSC) alebo zhrnutie vrátane počtu kontrolovaných cieľov, potvrdenia, že výsledky vyhovujú postupom kontroly PCI DSS a stavu súladu dokončeného ASV, musia byť odoslané spoločnosti American Express, aspoň raz za 90 dní.

Ak odosielate ROC AOC alebo STEP, nie ste povinní poskytnúť AOSC alebo zhrnutie kontroly ASV, pokiaľ to nie je výslovne vyžadované. Aby sa predišlo pochybnostiam, kontroly sú povinné, ak to vyžaduje príslušný SAQ.

**Osvedčenie STEP Overovacej dokumentácie (STEP) – (ročná požiadavka)** – STEP je k dispozícii iba pre Obchodníkov, ktorí spĺňajú kritériá uvedené v [Kroku 2: „Oboznámenie sa s Úrovňou Obchodníka/Poskytovateľa služieb a Požiadavkami na Overovaciu Dokumentáciu“](#) vyššie. Ak sa vaša spoločnosť kvalifikuje, musíte každoročne vyplniť a odoslať formulár Osvedčenia STEP spoločnosti American Express. Formulár Výročného Osvedčenia STEP je k dispozícii na stiahnutie z [Portálu](#). Môžete tiež kontaktovať svojho klientskeho manažéra alebo napísať spoločnosti American Express na adresu [AXPPCIComplianceProgram@aexp.com](mailto:AXPPCIComplianceProgram@aexp.com).

**Nesúlad s PCI DSS – (ročná, 90-dňová a/alebo ad hoc požiadavka)** – Ak nie ste v súlade s PCI DSS, musíte predložiť Súhrn nástrojov prioritného prístupu PCI (PAT) (k dispozícii na stiahnutie prostredníctvom webovej stránky Rady pre PCI Security Standards Council).

V Súhrne PAT musí byť uvedený dátum nápravy, ktorého termín nesmie byť neskôr ako dvanásť (12) mesiacov po dátume vyplnenia dokumentu, aby sa dosiahol súlad. Musíte poskytovať spoločnosti American Express pravidelné aktualizácie vášho pokroku smerom k náprave vášho stavu nesúladu (Obchodníci úrovne 1, úrovne 2, úrovne 3 a úrovne 4; všetci Poskytovatelia služieb). Nápravné opatrenia potrebné na dosiahnutie súladu s PCI DSS je potrebné vykonať na vaše náklady.

Spoločnosť American Express neuhradí poplatky za nedodržiavanie predpisov pred dátumom nápravy. Na základe [Tabuľky A-4 Poplatkov za nedodržiavanie predpisov](#) naďalej nesiete voči spoločnosti American Express zodpovednosť za všetky povinnosti súvisiace s odškodnením za Incidenty týkajúce sa údajov a vzťahujú sa na vás všetky ostatné ustanovenia týchto zásad.

Spoločnosť American Express si na základe vlastného uváženia ponecháva právo uložiť poplatky za nedodržiavanie predpisov, ak:

- nebola odoslaná Šablóna prioritného prístupu PCI v súlade s požiadavkami uvedenými v tomto oddiele,
- neboli splnené nápravné kroky uvedené v Šablóne prioritného prístupu PCI týkajúce sa stavu nesúlady,
- neboli splnené ktorékoľvek z požiadaviek Šablóny prioritného prístupu PCI týkajúce sa stavu nesúlady, alebo
- spoločnosti American Express nebola v príslušnom termíne alebo na jej žiadosť poskytnutá povinná dokumentácia o súlade.

Obchodníkom/Poskytovateľom služieb, ktorí nedodržia požiadavky uvedené v [Kroku 2: „Oboznámenie sa s Úrovňou Obchodníka/Poskytovateľa služieb a Požiadavkami na Overováciu Dokumentáciu“](#), môžu byť uložené poplatky, ako je uvedené v [Kroku 4: „Poslanie Overovacej dokumentácie spoločnosti American Express“](#).

**Aby sa predišlo pochybnostiam, Obchodníci, ktorí nedodržiavajú PCI DSS, nemajú nárok na zaradenie do Programu STEP.**

## Krok 4: Poslanie Overovacej dokumentácie spoločnosti American Express

Všetci Obchodníci a Poskytovatelia služieb, ktorí sú povinní zúčastniť sa na programe, musia spoločnosti American Express v príslušných termínoch predložiť Overováciu dokumentáciu označenú ako „povinné“ v tabuľkách v [Kroku 2: „Oboznámenie sa s Úrovňou Obchodníka/Poskytovateľa služieb a Požiadavkami na Overováciu Dokumentáciu“](#).

Musíte odoslať svoju Overováciu dokumentáciu spoločnosti American Express pomocou [Portálu](#) poskytovaného správcom Programu vybraným spoločnosťou American Express. Odoslaním Overovacej dokumentácie vyhlasujete a zaručujete spoločnosti American Express, že nasledovné je pravdivé (podľa vašich najlepších schopností):

- Vaše hodnotenie bolo úplné a dôkladné;
- Stav PCI DSS je presne znázornený v čase dokončenia, či už odosielate Osvedčenie o súlade (AOC) alebo Súhrn nástrojov prioritného prístupu PCI (PAT) pre nesúlad;
- Máte oprávnenie zverejniť informácie v nich obsiahnuté a poskytujete Overováciu dokumentáciu spoločnosti American Express bez toho, aby ste porušili práva akejkoľvek inej strany.

## Poplatky za nedodržiavanie predpisov a vypovedanie Dohody

Spoločnosť American Express má právo žiadať od vás zaplatať poplatkov za nedodržiavanie predpisov a vypovedať Dohodu, ak nespĺníte tieto požiadavky alebo ak do príslušného termínu neposkytnete spoločnosti American Express povinnú overovaciu dokumentáciu. Spoločnosť American Express sa pokúsi upozorniť kontakt na zabezpečenie údajov na príslušný termín pre každé ročné a štvrtročné obdobie podávania správ.

**Tabuľka A-4: Poplatok za nedodržiavanie predpisov**

| Popis*                                                                                                                                                                                                                                               | Obchodník 1. úrovne alebo Poskytovateľ služieb 1. úrovne | Obchodník 2. úrovne alebo Poskytovateľ služieb 2. úrovne | Obchodník 3. úrovne alebo 4. úrovne |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|-------------------------------------|
| Ak nedoručíte Overovaciu dokumentáciu do prvého termínu, stanoví sa poplatok za nedodržiavanie predpisov.                                                                                                                                            | 25 000 USD                                               | 5 000 USD                                                | 50 USD                              |
| Ak nedoručíte Overovaciu dokumentáciu do druhého termínu, stanoví sa dodatočný poplatok za nedodržiavanie predpisov.                                                                                                                                 | 35 000 USD                                               | 10 000 USD                                               | 100 USD                             |
| Ak nedoručíte Overovaciu dokumentáciu do tretieho termínu, stanoví sa dodatočný poplatok za nedodržiavanie predpisov.<br><b>POZNÁMKA:</b> Poplatky za nedodržiavanie predpisov budú naďalej účtované, kým nebude predložená Overovacia dokumentácia. | 45 000 USD                                               | 15 000 USD                                               | 250 USD                             |

\* Poplatky za nedodržiavanie predpisov sa budú posudzovať v ekvivalentoch v miestnej mene.

\* Neuplatňuje sa v Argentíne.

Ak vaše povinnosti týkajúce sa dokumentácie o súlade PCI DSS nie sú splnené, spoločnosť American Express bude oprávnená uložiť vám poplatky za nedodržiavanie predpisov kumulatívne, zadržať platby a/alebo vypovedať Dohodu.

## Oddiel 3

### Povinnosť spravovať Incidenty týkajúce sa údajov

Po zistení Incidentu týkajúceho sa údajov musíte okamžite, najneskôr však do sedemdesiatich dvoch (72) hodín upovedomiť spoločnosť American Express.

Spoločnosť American Express môžete upovedomiť prostredníctvom programu spoločnosti American Express na reakciu na incidenty (EIRP) na bezplatnom čísle 1 888 732 3750, alebo čísle 1 602 537 3021, alebo e-mailom na adrese [EIRP@aexp.com](mailto:EIRP@aexp.com). V prípade Incidentov týkajúcich sa údajov musíte určiť svoju kontaktnú osobu. Ďalej musíte:

- Každý Incident týkajúci sa údajov dôkladne forenzne vyšetriť a bezodkladne poskytnúť spoločnosti American Express všetky ohrozené Čísla kariet. Spoločnosť American Express si vyhradzuje právo uskutočniť vlastnú internú analýzu na zistenie údajov, na ktoré sa vzťahuje Incident týkajúci sa údajov.

V prípade Incidentov týkajúcich sa údajov, ktoré zahŕňajú menej ako 10 000 jedinečných Čísel kariet, musí byť spoločnosti American Express poskytnutý súhrn vyšetrovania do desiatich (10) pracovných dní po jeho dokončení.

- Súhrny vyšetrovania musia obsahovať nasledujúce informácie: súhrn incidentu, popis zasiahnutých prostredí, časovú os udalostí, kľúčové dátumy, podrobnosti o vplyve a ohrození údajov, opatrenia na obmedzenie a nápravu a potvrdenie, že neexistujú žiadne náznaky ohrozenia ďalších údajov spoločnosti American Express.

V prípade Incidentov týkajúcich sa údajov, ktoré zahŕňajú 10 000 alebo viac jedinečných Čísel kariet, musíte o vyšetrovanie požiadať Forenzného vyšetrovateľa pre oblasť PCI (PCI PFI), aby vykonal vyšetrovanie do piatich (5) dní od odhalenia Incidentu týkajúceho sa údajov.

- Neupravená správa o forenznom vyšetrovaní musí byť poskytnutá spoločnosti American Express do desiatich (10) pracovných dní po dokončení.
- Správy o forenznom vyšetrovaní sa musia vypracovať pomocou aktuálnej Šablóny konečnej forenznej správy o incidente, ktorú poskytuje PCI. Správa z forenzného vyšetrovania incidentu musí obsahovať forenzne preskúmania, správy o zhode a všetky ďalšie informácie súvisiace s Incidentom týkajúcim sa údajov; potvrdzovať, či ste v čase Incidentu týkajúceho sa údajov dodržiavali PCI DSS; a overiť vašu schopnosť predchádzať budúcim Incidentom týkajúcich sa údajov tak, že (i) budú obsahovať plán nápravy všetkých nedostatkov z hľadiska PCI DSS a (ii) zapojíte sa do programu dodržiavania predpisov spoločnosti American Express (ako je opísané nižšie). Na žiadosť spoločnosti American Express poskytnete potvrdenie Kvalifikovaného hodnotiteľa bezpečnosti (QSA) o náprave nedostatkov.

Bez ohľadu na vyššie uvedené odseky tohto [Oddielu 3. „Povinnosť spravovať Incidenty týkajúce sa údajov“](#):

- Spoločnosť American Express vás môže na základe vlastného uváženia požiadať, aby ste zapojili PFI, ktorý vykoná vyšetrovanie Incidentu týkajúceho sa údajov aj v prípade Incidentov zahŕňajúcich menej ako 10 000 jedinečných Čísel kariet alebo v prípade výskytu viacerých incidentov v rámci 12-mesačného obdobia. Každé takéto vyšetrovanie musí byť v súlade s požiadavkami stanovenými vyššie v tomto [Oddiele 3. „Povinnosť spravovať Incidenty týkajúce sa údajov“](#), a musí byť dokončené do uplynutia doby stanovenej spoločnosťou American Express.
- Spoločnosť American Express môže na základe vlastného uváženia samostatne zapojiť PFI, ktorý vykoná vyšetrovanie Incidentu týkajúceho sa údajov a môže vám zaúčtovať náklady takehoto vyšetrovania.

Musíte posúdiť Incident týkajúci sa údajov podľa príslušných zákonov o oznamovaní prípadov porušenia ochrany údajov na celosvetovej úrovni a v prípade potreby informovať príslušné regulačné orgány a dotknutých Držiteľov kariet v súlade s týmito zákonmi o oznamovaní prípadov porušenia ochrany údajov. Ak zistíte, že za oznámenie Incidentu týkajúceho sa údajov je zodpovedný váš Poskytovateľ služieb alebo iný subjekt, musíte daného Poskytovateľa služieb alebo subjekt upozorniť na jeho povinnosť posúdiť svoje oznamovacie povinnosti podľa príslušných zákonov o oznamovaní prípadov porušenia ochrany údajov. Súhlasíte, že pred uvedením alebo spomenutím spoločnosti American Express v akejkoľvek komunikácii s Držiteľmi kariet o Incidente týkajúcom sa údajov získate písomné schválenie od spoločnosti American Express. Ste povinní spolupracovať so spoločnosťou American Express na poskytnutí podrobností a náprave akýchkoľvek problémov vyplývajúcich z Incidentu týkajúceho sa údajov vrátane poskytnutia (a získania všetkých výnimiek potrebných na poskytnutie) všetkých relevantných informácií spoločnosti American Express, aby mohla overiť vašu schopnosť predchádzať budúcim Incidentom týkajúcich sa údajov spôsobom, ktorý je v súlade s Dohodou.

Spoločnosť American Express má bez ohľadu na akékoľvek protichodné povinnosti zachovania dôvernosti uvedené v Dohode právo zverejniť informácie o každom Incidente týkajúcom sa údajov Držiteľom kariet American Express, vydavateľom, ďalším účastníkom v sieti American Express a verejnosti v súlade s požiadavkami platných Právnych predpisov, na základe súdneho, správneho alebo regulačného príkazu, dekrétu, predvolania, žiadosti alebo v súvislosti s iným postupom s cieľom eliminovať riziko podvodu alebo inej ujmy v rozsahu primeranom na prevádzkovanie siete American Express.

## Čo robiť, ak u vás nastane Incident týkajúci sa údajov?

Ak ste vo svojej firme zistili Incident týkajúci sa údajov, postupujte podľa týchto krokov.



### Krok 1:

Vyplňte [Formulár prvotného oznámenia o Incidente obchodných údajov](#) a odošlite ho na adresu [EIRP@aexp.com](mailto:EIRP@aexp.com) do 72 hodín od zistenia Incidentu týkajúceho sa údajov.



### Krok 2:

Vykonajte dôkladné prešetrenie; môže sa vyžadovať, aby ste na to najali [Forenzného vyšetrovateľa pre oblasť Platobných kariet \(PCI\)](#).



### Krok 3:

Okamžite nám poskytnite všetky ohrozené čísla Kariet American Express®.



### Krok 4:

Spolupracujte s nami na riešení akýchkoľvek problémov vyplývajúcich z Incidentu týkajúceho sa údajov.

Ďalšie podrobnosti o povinnosti spravovať Incidenty týkajúce sa údajov nájdete v [Oddiele 3, „Povinnosť spravovať Incidenty týkajúce sa údajov“](#).

Máte viac otázok?

USA: (888) 732-3750 (bezplatné)

Medzinárodné: +1 (602) 537-3021

[EIRP@aexp.com](mailto:EIRP@aexp.com)

## Oddiel 4

### Povinnosti súvisiace s Odškodnením za Incident týkajúci sa údajov

V tomto [Oddiele 4, „Povinnosti súvisiace s Odškodnením za Incident týkajúci sa údajov“](#) sú definované vaše povinnosti súvisiace s odškodnením za Incidenty týkajúce sa údajov voči spoločnosti American Express podľa Dohody, pričom neznamenajú zrieknutie sa akýchkoľvek iných práv a nápravných prostriedkov spoločnosti American Express. Okrem vašich povinností súvisiacich s odškodnením (ak nejaké sú), sa na vás môže vzťahovať poplatok za nedodržiavanie predpisov súvisiacich s Incidentom týkajúcim sa údajov, ako je popísané nižšie v tomto [Oddiele 4, „Povinnosti súvisiace s Odškodnením za Incident týkajúci sa údajov“](#).

Odškodníte spoločnosť American Express sadzbou 5 USD za každé číslo účtu v prípade Incidentov týkajúcich sa údajov, ktoré zahŕňajú:

- 10 000 alebo viac Čísel kariet American Express a jednu alebo druhú z nasledujúcich podmienok:
  - Citlivé overovacie údaje, alebo
  - Dátum expirácie

Spoločnosť American Express však od vás nebude vyžadovať odškodnenie za Incidenty týkajúce sa údajov, ktoré zahŕňajú:

- menej ako 10 000 Čísel kariet American Express, alebo
- viac ako 10 000 Čísel kariet American Express, ak splníte nasledujúce podmienky:
  - upovedomili ste spoločnosť American Express o Incidente týkajúcom sa údajov podľa pokynov uvedených v [Oddiele 3, „Povinnosť spravovať Incidenty týkajúce sa údajov“](#),
  - dodržiavali ste v čase Incidentu týkajúceho sa údajov PCI DSS (podľa výsledkov vyšetrovania Incidentu týkajúceho sa údajov vedeného vyšetrovateľom PFI), a
  - Incident týkajúci sa údajov nevznikol v dôsledku vášho neoprávneného konania alebo konania Strán, ktoré zastupujete.

Bez ohľadu na vyššie uvedené odseky tohto [Oddielu 4. „Povinnosti súvisiace s Odškodnením za Incident týkajúci sa údajov“](#), v prípade akéhokoľvek Incidentu týkajúceho sa údajov a bez ohľadu na počet Čísel kariet American Express, zaplatíte spoločnosti American Express poplatok za nedodržanie predpisov súvisiacich s Incidentom týkajúcim sa údajov, ktorý nebude prevyšovať sumu 100 000 USD za každý Incident (stanovené podľa vlastného uváženia spoločnosti American Express) v prípade, že nedodržíte ktorúkoľvek z povinností stanovených v [Oddiele 3. „Povinnosť spravovať Incidenty týkajúce sa údajov“](#). Aby sa predišlo pochybnostiam, celkový poplatok za nedodržanie predpisov súvisiacich s Incidentom týkajúcim sa údajov za akýkoľvek jeden Incident neprevyšuje sumu 100 000 USD.

Spoločnosť American Express z kalkulácie vylúči akékoľvek Číslo účtu karty American Express, ktoré bolo v minulosti zahrnuté v nároku našej strany o odškodnenie za Incident týkajúci sa údajov do dvanástich (12) mesiacov od Dátumu upovedomenia. Všetky kalkulácie vykonané spoločnosťou American Express využitím tejto metodiky sú konečné.

Spoločnosť American Express vám môže zaúčtovať plnú sumu vašich povinností súvisiacich s odškodnením za Incidenty týkajúce sa údajov, alebo odpočítať túto sumu z platieb od spoločnosti American Express vám (alebo podľa toho zaťažiť váš Bankový Účet) v súlade s Dohodou.

Vaše povinnosti súvisiace s odškodnením za Incidenty týkajúce sa údajov uvedené v tomto dokumente sa podľa Dohody nepovažujú za náhodné, nepriame, špekulatívne, následné, špeciálne, trestné ani exemplárne škody za predpokladu, že tieto povinnosti nezahŕňajú škody súvisiace s ušlým ziskom alebo výnosmi, so stratou dobrého mena alebo so stratou obchodných príležitostí.

Spoločnosť American Express môže na základe vlastného uváženia znížiť povinnosť súvisiacu s odškodnením pre Obchodníkov, a to výlučne v prípade Incidentov týkajúcich sa údajov, ktoré spĺňajú všetky nasledujúce kritériá:

- pred Incidentom týkajúcim sa údajov a počas celého Obdobia trvania incidentu týkajúceho sa údajov sa používali príslušné Technológie na zníženie rizika,
- vykonalo sa dôkladné vyšetrovanie v súlade s programom PFI (ak sa predtým písomne nedohodlo inak),
- vo forenznej správe sa jasne uvádzajú Technológie na zníženie rizika, ktoré sa používali na spracovanie, ukladanie, a/alebo prenos údajov v čase Incidentu týkajúceho sa údajov, a
- neukladáte (a počas Obdobia trvania Incidentu týkajúceho sa údajov ste neukladali) Citlivé overovacie údaje ani žiadne Údaje o držiteľoch kariet, ktorých čitateľnosť sa neznemožnila.

V prípade, že existuje možnosť zníženia odškodného, zníženie vašej povinnosti súvisiacej s odškodnením (s výnimkou akýchkoľvek poplatkov za nedodržanie predpisov) sa určuje takto:

**Tabuľka A-5: Kritériá pre zníženie povinnosti súvisiacej s odškodnením**

| Zníženie povinnosti súvisiacej s odškodnením | Požadované kritériá                                                                                                                                                                                       |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Štandardné zníženie:<br>50 %                 | > 75 % z celkového počtu Transakcií bolo spracovaných v Zariadeniach s podporou čipov <sup>1</sup> ALEBO<br>vo > 75 % z Obchodníkových prevádzok sa používajú Technológie na zníženie rizika <sup>2</sup> |
| Rozsiahlejšie zníženie:<br>75 % až 100 %     | > 75 % z celkového počtu Transakcií bolo spracovaných v Zariadeniach s podporou čipov <sup>1</sup> A vo > 75 % z Obchodníkových prevádzok sa používa ďalšia z Technológií na zníženie rizika <sup>2</sup> |

<sup>1</sup> Podľa výsledkov internej analýzy spoločnosti American Express

<sup>2</sup> Podľa výsledkov vyšetrovania PFI

- Rozsiahlejšie zníženie (75 % až 100 %) sa stanoví na základe nižšej z percentuálnych hodnôt Transakcií spracovaných v Zariadeniach s podporou čipov A Obchodníkových prevádzok, v ktorých sa používa ďalšia z Technológií na zníženie rizika. Príklady v [Tabuľke A-6 Rozsiahlejšie zníženie povinnosti súvisiacej s odškodnením](#) ilustrujú kalkuláciu zníženia odškodného.
- Technológia sa považuje za Technológiu na zníženie rizika, ak preukážete jej účinné využívanie v súlade s jej koncepciou a zamýšľaným účelom.
- Percento prevádzok, v ktorých sa používa ďalšia z Technológií na zníženie rizika, sa určí podľa výsledkov vyšetrovania PFI.
- Zníženie povinnosti súvisiacej s odškodnením sa nevzťahuje na žiadne splatné poplatky za nedodržiavanie predpisov v súvislosti s Incidentom týkajúcim sa údajov.

**Tabuľka A-6: Rozsiahlejšie zníženie povinnosti súvisiacej s odškodnením**

| Príklad | Používané Technológie na zníženie rizika                                                                                                                                         | Nárok | Zníženie                                                                                                                                                  |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | <ul style="list-style-type: none"> <li>• 80 % Transakcií v Zariadeniach s podporou čipov</li> <li>• V 0 % prevádzok sa používa iná z Technológií na zníženie rizika</li> </ul>   | Nie   | 50 %: štandardné zníženie (pri používaní Technológií na zníženie rizika v menej ako 75 % prevádzok nevzniká nárok na rozsiahlejšie zníženie) <sup>1</sup> |
| 2       | <ul style="list-style-type: none"> <li>• 80 % Transakcií v Zariadeniach s podporou čipov</li> <li>• V 77 % prevádzok sa používa iná z Technológií na zníženie rizika</li> </ul>  | Áno   | 77 %: rozsiahlejšie zníženie (na základe používania Technológie na zníženie rizika v 77 % prevádzok)                                                      |
| 3       | <ul style="list-style-type: none"> <li>• 93 % Transakcií v Zariadeniach s podporou čipov</li> <li>• V 100 % prevádzok sa používa iná z Technológií na zníženie rizika</li> </ul> | Áno   | 93 %: rozsiahlejšie zníženie (na základe 93 % Transakcií v Zariadeniach s podporou čipov)                                                                 |
| 4       | <ul style="list-style-type: none"> <li>• 40 % Transakcií v Zariadeniach s podporou čipov</li> <li>• V 90 % prevádzok sa používa iná z Technológií na zníženie rizika</li> </ul>  | Nie   | 50 %: štandardné zníženie (pri menej ako 75 % Transakcií v Zariadeniach s podporou čipov nevzniká nárok na rozsiahlejšie zníženie)                        |

<sup>1</sup> Pri Incidente týkajúcom sa údajov vzťahujúcich sa na 10 000 účtov Kariet American Express so sadzbou 5,00 USD za každé číslo účtu (10 000 x 5 USD = 50 000 USD) môže vzniknúť nárok na zníženie o 50 %, čím sa povinnosť súvisiaca s odškodnením zníži z 50 000 USD na 25 000 USD s výnimkou akýchkoľvek poplatkov za nedodržiavanie predpisov.

## Oddiel 5

### Program cielenej analýzy (TAP)

Ohrozenie Údajov držiteľa karty môžu spôsobiť nedostatky v zabezpečení údajov vo vašom Prostredí údajov držiteľov kariet (CDE).

Medzi príklady ohrozenia Údajov držiteľa karty patria, okrem iného:

- **Spoločné miesto nákupu (CPP):** Držitelia kariet American Express ohlásia podvodné Transakcie na svojich Kartových účtoch a zároveň sa zistí, že vznikli pri nákupe vo vašich Prevádzkach.

- **Nájdene údaje Kariet:** Údaje Karty American Express a údaje Držiteľa karty sa nájdu na internete, s prepojením na Transakcie vo vašich Prevádzkach.
- **Podozrenie na malvér:** Spoločnosť American Express má podozrenie, že používate softvér, ktorý je infikovaný škodlivým kódom alebo je voči nemu zraniteľný.

Program TAP je určený na identifikáciu potenciálneho ohrozenia Údajov držiteľov kariet.

Musíte plniť a zabezpečiť, aby všetky Strany, ktoré zastupujete, plnili nasledujúce požiadavky po upozornení od spoločnosti American Express o možnom ohrození Údajov držiteľov kariet.

- Musíte urýchlene preveriť svoje CDE z hľadiska nedostatkov v bezpečnosti údajov a napraviť všetky zistenia.
  - V prípade outsourcingu musíte zabezpečiť, aby vaši predajcovia tretej strany dôkladne prešetrili vaše CDE.
- Na žiadosť spoločnosti American Express musíte poskytnúť súhrn podniknutých alebo plánovaných krokov previerky, posúdenia a/alebo nápravy.
- Musíte poskytnúť aktualizované overovacie dokumenty PCI DSS v súlade s [Oddielom 2. „Program dodržiavania predpisov PCI DSS \(dôležité periodické overovanie vašich systémov\)“](#).
- Podľa potreby musíte zamestnať kvalifikovaného PFI pre oblasť PCI, ktorý preskúma vaše CDE, pokiaľ vy alebo Strana, ktorú zastupujete:
  - Nedokáže vyriešiť narušenie bezpečnosti Údajov držiteľa karty v primeranej časovej lehote, podľa určenia spoločnosti American Express, alebo
  - Potvrdí, že Incident týkajúci sa údajov sa stal a dodrží požiadavky ustanovené v [Oddiele 3. „Povinnosť spravovať Incidenty týkajúce sa údajov“](#).

**Tabuľka A-7: Poplatok za nedodržiavanie TAP**

| Opis                                                                                                                                                                                                                                           | Obchodník 1. úrovne alebo Poskytovateľ služieb 1. úrovne | Obchodník 2. úrovne alebo Poskytovateľ služieb 2. úrovne | Obchodník 3. úrovne alebo 4. úrovne |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------|-------------------------------------|
| Poplatok za nedodržiavanie predpisov môže byť zvážení, keď nie sú povinnosti TAP splnené do prvého termínu.                                                                                                                                    | 25 000 USD                                               | 5 000 USD                                                | 1 000 USD                           |
| Poplatok za nedodržiavanie predpisov môže byť zvážení, keď nie sú povinnosti TAP splnené do druhého termínu.                                                                                                                                   | 35 000 USD                                               | 10 000 USD                                               | 2 500 USD                           |
| Poplatok za nedodržiavanie predpisov môže byť zvážení, keď nie sú povinnosti TAP splnené do tretieho termínu.<br><b>POZNÁMKA:</b> Poplatky za nedodržiavanie sa môžu uplatňovať naďalej, až do splnenia povinností alebo kým sa nevyrieši TAP. | 45 000 USD                                               | 15 000 USD                                               | 5 000 USD                           |

Ak nespĺníte svoje povinnosti podľa TAP, spoločnosť American Express bude oprávnená uložiť vám poplatky za nedodržiavanie predpisov kumulatívne, zadržať platby a/alebo vypovedať Dohodu.

## Oddiel 6

### Dôvernosť

Spoločnosť American Express prijme primerané opatrenia, aby zachovala (a primala svojich agentov a subdodávateľov vrátane Portálu, aby zachovávali) dôvernú vašich správ o dodržiavaní vrátane Overovacej dokumentácie a aby nezverejnila Overovaciu dokumentáciu žiadnej tretej strane (okrem pobočiek, agentov, zástupcov, Poskytovateľov služieb a subdodávateľov spoločnosti American Express) počas obdobia troch rokov

od dátumu prijatia, pričom táto povinnosť zachovania dôvernosti sa nevzťahuje na Overovaciu dokumentáciu, ktorá:

- a. je spoločnosti American Express známa už pred zverejnením;
- b. je alebo sa stane verejne známou bez toho, aby spoločnosť American Express porušila ustanovenie v tomto odseku;
- c. je spoločnosti American Express oprávnené odovzdaná treťou stranou bez povinnosti zachovania dôvernosti;
- d. je nezávisle vypracovaná spoločnosťou American Express; alebo
- e. musí byť zverejnená na základe príkazu súdu, správneho orgánu alebo vládneho orgánu, akéhokoľvek zákona, predpisu alebo nariadenia, na základe predvolania, výzvy na vyjadrenie, úradného predvolania alebo iného správneho či právneho postupu, prípadne na základe akéhokoľvek formálneho alebo neformálneho zisťovania alebo vyšetrovania akýmkoľvek vládny úradom alebo orgánom (vrátane akéhokoľvek regulačného orgánu, inšpektora, vyšetrovateľa alebo orgánu činného v trestnom konaní).

## Oddiel 7 Vyhlásenie o odmietnutí zodpovednosti

SPOLOČNOSŤ AMERICAN EXPRESS TÝMTO ODMIETA AKÉKOL'VEK A VŠETKY VYJADRENIA, ZÁRUKY A ZODPOVEDNOSŤ V SÚVISLOSTI S TÝMTO PREVÁDZKOVÝMI ZÁSADAMI TÝKAJÚCIMI SA BEZPEČNOSTI ÚDAJOV, PCI DSS, POŽIADAVKAMI EMV A URČOVANÍM A VÝKONOM QSA, ASV ALEBO PFI (ALEBO KTORÝCHKOĽVEK Z NICH), ČI UŽ EXPLICITNÉ, IMPLICITNÉ, ŠTATUTÁRNE, ALEBO INÉ VRÁTANE AKEJKOL'VEK ZÁRUKY OBCHODOVATEĽNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. VYDAVATELIA KARIET AMERICAN EXPRESS NIE SÚ PODĽA TÝCHTO ZÁSAD OPRÁVNENOU TREŤOU STRANOU.

## Oddiel 8 Glosár

Výlučne na účely týchto *Prevádzkových zásad týkajúcich sa bezpečnosti údajov* sa uplatňujú nasledujúce definície:

**Citlivé overovacie údaje** sú informácie súvisiace so zabezpečením, ktoré sa používajú na overenie držiteľov kariet a/alebo autorizáciu transakcií platobnými kartami. Tieto informácie zahŕňajú okrem iného overovacie kódy kariet, úplné stopové údaje (z magnetického prúžku alebo ekvivalentu na čipe), PIN kódy a PIN bloky.

**Čip** je integrovaný mikročip zabudovaný v Karte, ktorý obsahuje informácie o Držiteľovi karty a o účte.

**Čipová karta** je Karta, ktorá obsahuje Čip a ktorá by mohla vyžadovať zadanie kódu PIN na overenie identity Držiteľa karty alebo informácií o účte uložených v Čipe alebo oboch (v našich materiáloch sa niekedy označuje ako „smart karta“, „karta EMV“ alebo „ICC“, prípadne „karta s mikroprocesorom“).

**Číslo karty** je jedinečné identifikačné číslo, ktoré Vydavateľ prideliť Karte pri jej vydaní.

**Dátum upovedomenia** je dátum, keď spoločnosť American Express poskytne vydavateľom konečné upovedomenie o Incidente týkajúcom sa údajov. Tento dátum je podmienený dňom, keď spoločnosť American Express prijme konečnú forenznú správu alebo internú analýzu, a spoločnosť American Express tento dátum určí na základe vlastného uváženia.

**Dohoda** znamená súhrne Všeobecné ustanovenia, Nariadenia pre Obchodníkov a všetky sprievodné plány a prílohy (v našich materiáloch sa niekedy označuje ako Dohoda o akceptácii kariet).

**Držiteľ karty** je jednotlivец alebo subjekt, (i) ktorý s vydavateľom uzavrel dohodu, ktorou sa zriaďuje účet Karty, alebo (ii) ktorého meno sa uvádza na Karte.

**Držiteľ karty** je zákazník, ktorému je vydaná platobná karta, alebo ľubovoľná osoba oprávnená používať platobnú kartu.

**Forenzný vyšetrovateľ pre oblasť PCI (PFI)** je subjekt, ktorý Rada Payment Card Industry Security Standards Council, LLC, poverila vykonávaním forenzných vyšetrovaní v prípade porušenia ochrany alebo ohrozenia Údajov o platobných kartách.

**Franchisant** je tretia strana s nezávislým vlastníctvom a prevádzkou (vrátane franchisanta, nadobúdateľa licencie alebo skupiny), okrem Pobočky, ktorá má udelenú licenciu od Franchisora na prevádzkovanie franchise

a uzavrela písomnú zmluvu s Franchisorom, na základe ktorej dôsledne preukazuje vonkajšiu identifikáciu, ktorou vyjadruje identifikáciu so Značkami Franchisora, alebo sa prezentuje verejnosti ako člen skupiny spoločností Franchisora.

**Franchisor** je prevádzkovateľ spoločnosti, ktorý udeľuje osobám alebo Subjektom (Franchisantom) licencie, aby mohli distribuovať tovar a/alebo služby pod Značkou prevádzkovateľa alebo pod ňou fungovať; poskytujú Franchisantom pomoc pri prevádzkovaní ich spoločností alebo ovplyvňuje spôsob fungovania Franchisantov a od Franchisantov vyžaduje úhradu poplatku.

**Incident týkajúci sa údajov** je incident, pri ktorom došlo k ohrozeniu alebo k podozreniu z ohrozenia šifrovaných kľúčov spoločnosti American Express alebo aspoň jedného čísla účtu Karty American Express, pričom došlo k:

- neoprávnenému prístupu k Šifrovaným kľúčom, Údajom o držiteľoch kariet alebo Citlivým overovacím údajom (alebo ich kombinácii) uloženým, spracovávaným alebo prenášaným v zariadeniach, systémoch alebo sieťach (alebo ich súčiastkach), ktoré sú vaše alebo ktorých používaním poverujete ďalšie strany, ktoré poskytujete alebo sprístupňujete, alebo došlo k použitiu týchto údajov;
- inému použitiu Šifrovaných kľúčov, Údajov o držiteľoch kariet alebo Citlivých overovacích údajov (alebo ich kombinácii) v rozpore s Dohodou; a/alebo
- podozreniu zo straty, krádeže alebo sprenevery alebo k potvrdenej strate, krádeži alebo sprenevere akýmkoľvek spôsobom a využitím akýchkoľvek médií, materiálov, záznamov alebo informácií obsahujúcich takéto Šifrovacie kľúče, Údaje o držiteľoch kariet alebo Citlivé overovacie údaje (alebo ich kombináciu).

**Informácie o Držiteľoch kariet** sú informácie o Držiteľoch kariet a Transakciách kartami American Express vrátane mien, adries, čísel účtov kariet a identifikačných čísel kariet (CID).

**Karta American Express**, alebo **Karta**, je akákoľvek karta, zariadenie na prístup k účtu alebo platobné zariadenie alebo služba, ktorá nesie názov, logo, ochrannú známku, ochrannú známku pre služby, obchodný názov alebo akýkoľvek iný vlastný dizajn alebo označenie spoločnosti American Express alebo jej pobočky a ktorú vydal vydavateľ alebo číslo účtu karty.

**Kvalifikovaný hodnotiteľ bezpečnosti (QSA)** je subjekt, ktorému Rada Payment Card Industry Security Standards Council, LLC udelila oprávnenie overovať dodržiavanie PCI DSS.

**Obchodník** je Obchodník a všetky jeho pobočky, ktoré prijímajú Karty American Express podľa Dohody so spoločnosťou American Express alebo s jej pobočkami.

**Obchodník 1. úrovne** je Obchodník s 2,5 miliónom Transakcií alebo viac kartami American Express ročne alebo akýkoľvek Obchodník, ktorého spoločnosť American Express považuje za Obchodníka 1. úrovne.

**Obchodník 2. úrovne** je Obchodník, ktorý má 50 000 až menej ako 2,5 milióna Transakcií kartami American Express ročne.

**Obchodník 3. úrovne** je Obchodník, ktorý má 10 000 až menej ako 50 000 Transakcií kartami American Express ročne.

**Obchodník 4. úrovne** je Obchodník, ktorý má menej ako 10 000 Transakcií kartami American Express ročne.

**Obdobie trvania Incidentu týkajúceho sa údajov** je obdobie narušenia (alebo podobne určené časové obdobie), určené v záverečnej forenznnej správe (napr. správe PFI), alebo ak nie je známe, do 365 dní pred posledným Dátumom upovedomenia o číslach potenciálne kompromitovaných Kariet zasiahnutých ohrozením údajov, ktoré nám bolo oznámené.

**Ohrozené číslo karty** je číslo účtu Karty American Express súvisiace s Incidentom týkajúcim sa údajov.

**Osvedčenie o súlade (AOC)** je vyhlásenie o vašom stave dodržiavania PCI DSS vo formulári poskytnutom Radou Payment Card Industry Security Standards Council, LLC.

**Osvedčenie o súlade s požiadavkami na kontrolu (AOSC)** je vyhlásenie o vašom stave dodržiavania PCI DSS na základe kontroly siete, a to vo formulári poskytnutom Radou Payment Card Industry Security Standards Council, LLC.

**Overovacia dokumentácia** zahŕňa AOC poskytnuté v súvislosti s Výročným bezpečnostným hodnotením na mieste alebo SAQ, AOSC a zhrnutia výsledkov poskytnuté v súvislosti so Štvrťročnými kontrolami siete alebo výročné osvedčenie Programu na posilnenie bezpečnostných technológií.

**Payment Card Industry Data Security Standard (PCI DSS)** je Norma týkajúca sa bezpečnosti údajov pre odvetvie platobných kariet, ktorá je dostupná na adrese [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**PCI DSS** je Norma týkajúca sa bezpečnosti údajov pre odvetvie platobných kariet, ktorá je dostupná na adrese [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Platba** je platba alebo nákup uskutočnený pomocou Karty.

**Platobná aplikácia** má význam, ktorý stanovuje aktuálny Glosár pojmov pre Normu týkajúcu sa bezpečnosti softvéru a Normu pre bezpečný životný cyklus softvéru v odvetví platobných kariet, ktorý je dostupný na adrese [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Platobný systém v mieste predaja (POS)** je systém alebo zariadenie na spracovanie informácií vrátane terminálu, osobného počítača, elektronickej registračnej pokladne, bezkontaktnéj čítačky, alebo platobného nástroja, alebo postupu, ktorý Obchodník používa na získavanie oprávnení alebo zhromažďovanie údajov o Transakciách alebo pre obidva účely.

**Portál** znamená systém hlásení poskytovaný správcom Programu American Express PCI, ktorý vybrala spoločnosť American Express. Obchodníci a Poskytovatelia služieb sú povinní používať Portál na odosielanie overovacej dokumentácie PCI spoločnosti American Express.

**Poskytovatelia služieb** sú oprávnení spracovatelia, spracovatelia ako tretie strany, poskytovatelia brán, integrátori Systémov POS a všetci ďalší poskytovatelia, ktorí Obchodníkom poskytujú Systémy POS alebo iné riešenia či služby na spracovanie platieb.

**Poskytovateľ služieb 1. úrovne** je Poskytovateľ služieb s 2,5 miliónom a viac Transakciami kartami American Express ročne alebo akýkoľvek Poskytovateľ služieb, ktorého spoločnosť American Express považuje za Poskytovateľa služieb 1. úrovne.

**Poskytovateľ služieb 2. úrovne** je Poskytovateľ služieb, ktorý má menej ako 2,5 milióna Transakcií kartami American Express ročne alebo akýkoľvek Poskytovateľ služieb, ktorého spoločnosť American Express nepovažuje za Poskytovateľa služieb 1. úrovne.

**Požiadavky EMV** sú požiadavky vydané spoločnosťou EMVCo, LLC, ktoré sú dostupné na adrese [www.emvco.com](http://www.emvco.com).

**Požiadavky Rady Payment Card Industry Security Standards Council (PCI SSC)** sú súbor noriem a požiadaviek, týkajúcich sa zabezpečenia a ochrany údajov o platobných kartách, vrátane PCI DSS a PA DSS, dostupných na [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Požiadavky zabezpečenia prostredníctvom kódu PIN pre oblasť PCI** sú požiadavky zabezpečenia prostredníctvom kódu PIN v odvetví platobných kariet, ktoré sú dostupné na adrese [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Primárne číslo účtu (PAN)** má význam daný vo vtedy aktuálnom glosáre pojmov pre PCI DSS.

**Program** znamená Program dodržiavania predpisov PCI spoločnosti American Express.

**Program cielenej analýzy** znamená program, ktorý zabezpečuje včasnú identifikáciu potenciálneho ohrozenia údajov držiteľa karty vo vašom Prostredí údajov o držiteľoch kariet (CDE). Pozri [Oddiel 5, „Program cielenej analýzy \(TAP\)“](#).

**Program na posilnenie bezpečnostných technológií (STEP)** je program spoločnosti American Express, ktorý Obchodníkov podporuje, aby nasadzovali technológie zlepšujúce zabezpečenie údajov.

**Prostredie údajov o držiteľoch kariet (CDE)** zahŕňa ľudí, procesy a technológie, ktoré uchovávajú, spracúvajú alebo prenášajú údaje držiteľov kariet alebo citlivé autentifikačné údaje.

**Refundácia** je suma z Platby, ktorú refundujete Držiteľom kariet za nákupy alebo platby uskutočnené pomocou Karty.

**Samohodnotiaci dotazník (SAQ)** je nástroj samohodnotenia vytvorený Radou Payment Card Industry Security Standards Council, LLC, ktorý má slúžiť na hodnotenie a osvedčovanie súladu s PCI DSS.

**Schválené riešenie šifrovania Point-to-Point (P2PE)**, zahrnuté v zozname schválených riešení PCI SSC alebo schválené spoločnosťou P2PE, ktorá je kvalifikovaným hodnotiteľom bezpečnosti PCI SSC.

**Schválený kontrolór (ASV)** je Subjekt, ktorému Rada Payment Card Industry Security Standards Council, LLC, udelila oprávnenie overovať dodržiavanie určitých požiadaviek PCI DSS uskutočňovaním kontroly zraniteľnosti prostredím pripojených na internet.

**Schválený pre oblasť PCI** znamená, že Zariadenie so zadávaním kódu PIN alebo Platobná aplikácia (alebo obe) sú v čase nasadenia uvedené v zozname schválených spoločností a poskytovateľov, ktorý aktualizuje Rada PCI Security Standards Council, LLC, a ktorý je dostupný na adrese [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Spracovateľ** je poskytovateľ služieb Obchodníkom, ktorý uľahčuje spracovanie oprávnení a odosielanie správ v sieti American Express.

**Strany, ktoré zastupujete**, sú ľubovoľní alebo všetci vaši zamestnanci, agenti, zástupcovia, subdodávatelia, Spracovatelia, Poskytovatelia služieb, poskytovatelia vášho vybavenia, systémov alebo riešení na spracovanie platieb v mieste predaja (POS), subjekty súvisiace s vašim účtom Obchodníka American Express a akákoľvek iná strana, ktorej môžete v súlade s Dohodou poskytovať prístup k Údajom o Držiteľoch kariet alebo Citlivým overovacím údajom (prípadne oboje).

**Šablóna konečnej forenzej správy o incidente** znamená šablónu dostupnú od PCI Security Standards Council, ktorá je dostupná na [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Šifrovací kľúč („šifrovací kľúč American Express“)** predstavuje všetky kľúče použité pri spracúvaní, generovaní, načítavaní alebo ochrane údajov o účte. To zahŕňa okrem iného tieto kľúče:

- Kľúče na šifrovanie kľúčov: Zone Master Key (ZMK) a Zone Pin Key (ZPK)
- Kľúče Master Key používané v zabezpečených kryptografických zariadeniach: Local Master Key (LMK)
- Kľúče Card Security Code Key (CSCK)
- Kľúče s kódom PIN: Base Derivation Key (BDK), PIN Encryption Key (PEK) a ZPK

**Šifrovanie Point-to-Point (P2PE)** je riešenie, ktoré kryptograficky chráni údaje o účte od chvíle, keď obchodník prijme platobnú kartu, do chvíle, keď dôjde k bezpečnému dešifrovaniu.

**Spotrebiteľ** je definovaný ako držiteľ karty kupujúci tovar, služby alebo oboje.

**Technológia na zníženie rizika** sú technologické riešenia, ktoré zvyšujú zabezpečenie Údajov o držiteľoch kariet American Express a Citlivých overovacích údajov stanovené spoločnosťou American Express. Technológia sa považuje za Technológiu na zníženie rizika, ak preukážete jej účinné využívanie v súlade s jej koncepciou a zamýšľaným účelom. Príklady zahŕňajú ale nie sú obmedzené na: EMV, šifrovanie Point-to-Point a tokenizáciu.

**Token** znamená kryptografický token, ktorý nahrádza PAN na základe daného indexu pre nepredvídateľnú hodnotu.

**Transakcia** je Platba, Refundácia, Výber Hotovosti (alebo iný prístup k hotovosti) alebo Bankomatová Transakcia uskutočnená pomocou Karty.

**Transakcia EMV** je Transakcia kartou s mikroprocesorom (niekedy označovanou ako „karta IC“, „čipová karta“, „smart karta“, „karta EMV“ alebo „ICC“) vykonaná na termináli v mieste predaja (POS) s platným a aktuálnym schválením typu EMV. Schválenia typu EMV sú dostupné na adrese [www.emvco.com](http://www.emvco.com).

**Transakcie súvisiace s platbami iniciovanými kupujúcimi (BIP)** predstavujú riešenie digitálnych platieb, ktoré umožňuje kupujúcim rýchlo a efektívne plánovať platby dodávateľom (prepojené s firemnými kartami).

**Údaje držiteľa karty** zahŕňajú minimálne úplné Primárne číslo účtu (PAN) samostatne alebo úplné PAN spolu s ktorýmkoľvek z nasledujúcich údajov: meno držiteľa karty, dátum expirácie a/alebo kód služby. Pozrite si

pojem Citlivé overovacie údaje, pri ktorom sú uvedené ďalšie prvky údajov, ktoré sa môžu prenášať alebo spracovávať (ale nie uchovávať) v rámci platobnej transakcie.

**Údaje o Transakciách** sú všetky informácie požadované spoločnosťou American Express, ktoré preukazujú jednu alebo viac Transakcií, vrátane informácií získaných v mieste predaja, informácií získaných alebo vygenerovaných počas Autorizácie a Odoslania a akejkoľvek Spätnej Úhrady.

**Údaje o účte** zahŕňajú Údaje držiteľa karty a/alebo citlivé overovacie údaje. Pozrite si pojmy Údaje držiteľa karty a Citlivé overovacie údaje.

**Úroveň Obchodníka** znamená označenie, ktoré prideliťme Obchodníkom v súvislosti s ich povinnosťami overovania súladu s PCI DSS, ako je popísané v [Oddiele 2, „Program dodržiavania predpisov PCI DSS \(dôležité periodické overovanie vašich systémov\)“](#).

**Vydavateľ Kariet** je akýkoľvek Subjekt (vrátane spoločnosti American Express a jej Pobočky), licenciou udelenou spoločnosťou American Express alebo Pobočkou American Express na vydávanie Kariet a účasť na podnikaní v oblasti vydávania Kariet.

**Zariadenie so zadávaním kódu PIN** má význam, ktorý stanovuje Glosár pojmov pre bezpečnosť transakcií pomocou kódu PIN (PTS) odvetvia platobných kariet v mieste interakcií (POI) – modulárne bezpečnostné požiadavky – ktorý je dostupný na adrese [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Zariadenie s podporou čipov** je zariadenie v mieste predaja, ktoré má platné a aktuálne schválenie/certifikát EMVCo ([www.emvco.com](http://www.emvco.com)) a ktoré dokáže spracovávať Transakcie Čipovými kartami v súlade s AEIPS.

**Záznam o Platbe** je reprodukovateľný (papierový aj elektronický) záznam o Platbe, ktorý spĺňa naše požiadavky a obsahuje Číslo Karty, Dátum transakcie, sumu v dolároch, Schválenie, podpis Držiteľa karty (ak je to relevantné) a ďalšie informácie.

**Záznam o Refundácii** je záznam o Refundácii, ktorý spĺňa naše požiadavky.

## Oddiel 9

### Užitočné webové stránky

Zabezpečenie údajov spoločnosti American Express: [www.americanexpress.com/datasecurity](http://www.americanexpress.com/datasecurity)

PCI Security Standards Council, LLC: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

EMVCo: [www.emvco.com](http://www.emvco.com)