

Andmeturbe Tegevuspoliitika (DSOP)

Peatükk 1	DSOP ja Turbestandardite Sissejuhatus	3
Peatükk 2	PCI DSS Vastavusprogramm (teie Süsteemide Oluline Perioodiline Valideerimine)	3
Meede 1:	Osalege American Expressi Vastavusprogrammis selle Poliitika alusel	4
Meede 2:	Teadke oma Kaupmehe/Teenusepakkuja Taset ja Valideerimise Dokumentide Nõudeid	4
Meede 3:	Täitke Valideerimise Dokumendid, mille peate saatma American Expressile	7
Meede 4:	Saatke Valideerimise Dokumendid American Expressile	9
Peatükk 3	Andmeintsidentide Haldamise Kohustused	10
Peatükk 4	Hüvitamiskohustused Andmeintsidendi Korral	12
Peatükk 5	Sihtanalüüsi programm (Targeted Analysis Programme, TAP)	14
Peatükk 6	Konfidentsiaalsus	15
Peatükk 7	Vastutuse piirang	16
Peatükk 8	Sõnastik	16
Peatükk 9	Kasulikud veebisaidid	20

DSOP Muudatuste Kokkuvõte

Ikoonid

Tähtsad uuendused on loetletud Muudatuste Kokkuvõtte Tabelis ja märgistatud ka *DSOP-is* muudatuste ribaga. Muudatuste riba on vertikaalne joon, enamasti vasakul veerisel, mis tähistab lisatud või muudetud teksti. Ainult olulised *DSOP-i* muudatused, mis võivad mõjutada Kaupmehe toiminguid, on toodud muudatuste ribal, mis on kuvatud vasakul veerisel.



Eemaldatud tekst on märgistatud prügikasti ikooniga, mis on paigutatud veerisele olulise tekstieemalduse kõrvale, sealhulgas peatükid, tabelid, jaotised, märkused ja loetelupunktid. Eemaldatud tekstile viidatakse käesolevas Muudatuste Kokkuvõttes, kasutades eelmise väljaande jaotiste nummerdust, vältimaks segadust.

Sinised jooned jaotiste ümber viitavad piirkonnaspetsiifilisele infole.

Muudatuste Kokkuvõtte Tabel

Tähtsad uuendused on loetletud järgmises tabelis ja märgistatud ka *DSOP-is* muudatuste ribaga.

Peatükk/Alapeatükk	Muudatuste kirjeldus
Selles versioonis pole muudatusi.	

Peatükk 1 DSOP ja Turbestandardite Sissejuhatus

Tarbijakaitset esikohale seadva ettevõtteks on American Express pikaajaliselt pühendunud Kaardiomanike Andmete ja Tundlike Autentimise Andmete kaitsmisele ning nende turvalisuse tagamisele.

Kompromiteeritud andmed mõjutavad negatiivselt tarbijaid, Kaupmehi, Teenusepakkujaid ja kaardi väljastajaid. Isegi üks vahejuhtum võib äriühingu mainet oluliselt rikkuda ja kahjustada selle võimet efektiivsele äritegevusele. Selle ohuga tegelemine andmeturbe tegevuspoliitikate rakendamise teel võib aidata parandada klientide usaldust, suurendada kasumlikkust ja parendada äriühingu mainet.

American Express teab, et meie Kaupmehed ja Teenusepakkujad (ühiselt kui: teie) jagavad meie muret, ja vajab osana teie kohustustest, et te järgiksite oma lepingus olevaid andmeturbe sätteid, et võtta vastu (Kaupmeeste puhul) või töödelda (Teenusepakkujate puhul) American Express®-i Kaarti (igaüks vastavalt kui: **Leping**) ja seda Andmeturbe Tegevuspoliitikat (DSOP), mida meil on õigus aeg-ajalt muuta. Käesolevad nõuded rakenduvad kõigile teie seadmetele, süsteemidele ja võrkudele (ning nende osadele), millel Krüpteerimisvõtmed, Kaardiomaniku Andmed või Tundlikud Autentimise Andmed (või nende kombinatsioon) on talletatud, töödeldud või edastatud.

Suure algustähega kasutatud, kuid siinkohal defineerimata terminite tähendused on välja toodud käesoleva poliitika lõpus olevas sõnastikus.

Andmeturbe Tegevuspoliitika (DSOP) on kõikehõlmav nõuete poliitika, mis on mõeldud Konto Andmete kaitsmiseks nende andmete salvestamisel, töötlemisel või edastamisel.

American Express nõuab kõikidelt Kaupmeestelt ja Teenusepakkujatelt vastamist Maksekaarditööstuse Andmeturbestandardile (PCI DSS). Nende nõuete hulka kuulub, et teie ja teie Seotud Pooled peate:

- Talletama Kaardiomaniku Andmeid üksnes selleks, et võimaldada American Expressi Kaardi Tehinguid kooskõlas Lepinguga ja vastavalt Lepingus nõutule.
- Tagama kooskõla hetkel kehtiva Maksekaarditööstuse Andmeturbestandardi (Payment Card Industry Data Security Standard, PCI DSS) Nõuetega, mida kohaldatakse teie Kaardiomanike Andmete või Tundlike Autentimise Andmete töötlemisele, talletamisele või edastamisele hiljemalt kohaldatava nõude selle versiooni rakendamise kuupäevaks.
- Tagama PCI-le vastavate toodete kasutamise andmete salvestamise, töötlemise või edastamise tehnoloogia rakendamisel või asendamisel.

Te peate kaitsma kõiki American Expressi Tasu- ja Krediidandmeid, mida Lepingu kohaselt säilitatakse kooskõlas käesolevate andmeturbe sätetega. Te peate kasutama neid andmeid ainult Lepingus sätestatud eesmärkidel ja neid vastavalt kaitsma. Te vastutate American Expressi ees nii rahaliselt kui ka mis tahes muul moel, tagamaks, et teie Seotud Poolte tegevus on käesolevate andmeturbe sätetega kooskõlas (välja arvatud juhul, kui näitate oma Seotud Poolte vastavust käesoleva poliitika jaole [Peatükk 2. "PCI DSS Vastavusprogramm \(teie Süsteemide Oluline Perioodiline Valideerimine\)"](#), kui selles peatükis ei ole sätestatud teisiti). Üksikasjaliku info PCI standardite kohta ja nõuetele vastamise tagamise kohta leiate veebisaidilt www.pcisecuritystandards.org.

Peatükk 2 PCI DSS Vastavusprogramm (teie Süsteemide Oluline Perioodiline Valideerimine)

Te peate läbima järgmised meetmed, et kinnitada PCI DSSi alusel kord aastas ja iga 90 päeva järel, nagu on kirjeldatud allpool, teie ja teie Volitatud Edasimüüjate seadmete, süsteemide ja/või võrgustike (ning nende komponentide) olek, kus Kaardiomaniku Andmeid või Tundlike Autentimise Andmeid talletatakse, töödeldakse või edastatakse.

Need on neli meetet, mis on kinnituse täitmiseks vaja:

- [Meede 1](#): Osalege American Expressi PCI vastavusprogrammis selle poliitika kohaselt.
- [Meede 2](#): Teadke oma Kaupmehe/Teenusepakkuja Taset ja Valideerimise Dokumentide Nõudeid.
- [Meede 3](#): Täitke Valideerimise Dokumendid, mille peate American Expressile saatma.
- [Meede 4](#): Saatke Valideerimise Dokumendid ettenähtud ajavahemikus American Expressile.

Meede 1: Osalege American Expressi Vastavusprogrammis selle Poliitika alusel

1. taseme Kaupmehed, 2. taseme Kaupmehed ja kõik Teenusepakkujad, nagu on kirjeldatud allpool, peavad osalema Programmis vastavalt sellele poliitikale. American Express võib määrata omal äranägemisel kindlad 3. taseme ja 4. taseme Kaupmehed, kes osalevad selle poliitika alusel Programmis.

Programmis osalema peavad Kaupmehed ja Teenusepakkujad peavad ette nähtud ajavahemiku jooksul registreerima American Expressi valitud Programmiadministraatori pakutud Portaalis.

- Te peate nõustuma kõigi vastuvõetavate tingimustega, mis on seotud Portaali kasutamisega.
- Te peate sisestama ja esitama täpse teabe vähemalt ühe andmeturbe kontakti kohta Portaalis. Nõutav info hõlmab järgmist:
 - Täisnimi
 - E-posti aadress
 - Telefoninumber
 - Füüsiline postiaadress
- Te peate esitama uuendatud või uue kontaktteabe sisestatud andmeturbe kontakti kohta Portaalis, kui see teave muutub.
- Te peate tagama, et teie süsteemid on ajakohased sideteenuste osutamiseks Portaali määratud domeenist.

Kui te ei suuda tagada või säilitada ajakohast andmeturbe kontaktteavet ega võimaldada e-posti sidet, ei mõjuta see meie õigust küsida tasu.

Meede 2: Teadke oma Kaupmehe/Teenusepakkuja Taset ja Valideerimise Dokumentide Nõudeid

Olemas on neli Kaupmehe Taset, mis kehtib Kaupmeestele ja Teenusepakkujatele kohalduvale kahele tasemele vastavalt teie American Expressi Kaarditehingute mahule.

- Kaupmeeste puhul on see maht, mille on lisanud nende Ettevõtted, mis registreeruvad kuni kõige kõrgema American Expressi Kaupmehe kontotasemel.*
- Teenusepakkujate puhul on see mahu summa, mille on esitanud Teenusepakkuja ja Ettevõtete Teenusepakkuja, kellele te teenuseid osutate.

Määratledes Kaupmehe Taset ja valideerimise nõudeid, ei arvestata Ostja Algatatud Makse (Buyer Initiated Payments, BIP) Tehinguid American Expressi Kaardi Tehingute hulka. Teid liigitatakse ühele Kaupmehe tasemele, mis on määratletud [Tabel A-1: Kaupmehe ja Teenusepakkuja Tasemed](#).

* Frantsiisiandjate puhul sisaldab see nende Frantsiisivõtja Ettevõtetest tulenevat hulka. Frantsiisiandjad, kes määravad kindlaks, et nende Frantsiisivõtjad kasutaksid kindlat Müügikohapõhist ehk POS-Süsteemi või -Teenusepakkujat, peavad esitama ka mõjutatud Frantsiisivõtjate valideerimise dokumendid.

Tabel A-1: Kaupmehe ja Teenusepakkuja Tasemed

Kaupmehe/Teenusepakkuja Tase	Iga-aastased American Expressi Tehingud
1. taseme Kaupmees	2,5 miljonit või enam American Expressi Kaardi Tehingut aastas; või mis tahes muu Kaupmees, kellele American Express määrab omal äranägemisel 1. taseme.
2. taseme Kaupmees	50 000 kuni alla 2,5 miljonit American Expressi Kaardi Tehingut aastas.
3. taseme Kaupmees	10 000 kuni alla 50 000 American Expressi Kaardi Tehingut aastas.
4. taseme Kaupmees	Alla 10 000 American Expressi Kaardi Tehingut aastas.
Teenusepakkuja Tase	Iga-aastased American Expressi Tehingud
1. taseme Teenusepakkuja	2,5 miljonit või enam American Expressi Kaardi Tehingut aastas; või mis tahes Teenusepakkuja, kelle American Express määrab 1. tasemele.
2. taseme Teenusepakkuja	alla 2,5 miljonit American Expressi Kaardi Tehingut aastas; või mis tahes Teenusepakkuja, keda American Express pole määranud 1. tasemele.

Kaupmehe Valideerimise Dokumentide Nõuded

Kaupmeestel (mitte Teenusepakkujatel) on neli võimalikku Kaupmehe Taseme Klassifikatsiooni. Pärast Kaupmehe Taseme määramist [Tabel A-1: Kaupmehe ja Teenusepakkuja Tasemed](#) alusel (eespool), vt [Tabel A-2: Kaupmehe Valideerimise Dokumentid](#), et selgitada välja dokumentatsiooni nõuded.

Tabel A-2: Kaupmehe Valideerimise Dokumentid

Kaupmehe tase / Iga-aastased American Expressi tehingud	Aruanne Vastavuse Atesteerimise kohta (ROC AOC)	Vastavuse Atesteerimise Küsimustik (SAQ AOC) JA Kvartaalne Välisvõrgustik Haavatavuse Analüüs (analüüs)	Turbetehnoloogia Parandamise Programmi (STEP) atesteerimine kirt eeriumitele vastavate Kaupmeeste puhul
1. tase / 2,5 miljonit või enam	Kohustuslik	Ei ole kohaldatav	Valikuline American Expressi heakskiiduga (asendab ROC)
2. tase/ 50 000 kuni alla 2,5 miljoni	Valikuline	SAQ AOC kohustuslik (kui ei esitata ROC AOC); analüüs kohustuslik teatud SAQ tüüpide puhul	Valikuliselt koos American Expressi heakskiiduga* (asendab SAQ ja võrgu analüüsi või ROC)
3. tase**/ 10 000 kuni alla 50 000	Valikuline	SAQ AOC valikuline (kohustuslik, kui seda nõuab American Express); analüüs kohustuslik teatud SAQ tüüpide puhul	Valikuliselt koos American Expressi heakskiiduga* (asendab SAQ ja võrgu analüüsi või ROC)
4. tase**/ Alla 10 000	Valikuline	SAQ AOC valikuline (kohustuslik, kui seda nõuab American Express); analüüs kohustuslik teatud SAQ tüüpide puhul	Valikuliselt koos American Expressi heakskiiduga* (asendab SAQ ja võrgu analüüsi või ROC)

* **Märkus:** American Express PCI meeskond vaatab üle taotluse ja kriteeriumitele vastavuse ning kinnitab, kui te kvalifitseerute STEP programmi jaoks. Kriteeriumitele vastavuse kontrollimiseks võtke ühendust Kliendihalduriga ja/või e-posti aadressil AXPCComplianceProgram@aexp.com.

**Kahtluste vältimiseks ei pea 3. ja 4. taseme Kaupmehed esitama Valideerimise Dokumente, kui American Express seda omal äranägemisel ei nõua, kuid peab sellele siiski vastama ja on kohustatud vastama kõigile teistele selle Andmeturbe Tegevuspoliitika sätetele.

American Express jätab endale õiguse kontrollida teie PCI Valideerimise Dokumentide terviklikkust, täpsust ja asjakohasust. American Express võib paluda teil esitada täiendavaid tugidokumente, et hinnata selle eesmärgi toetamist. Lisaks on American Expressil õigus nõuda, et te rakendaksite PCI Turbestandardi nõukogu heakskiidetud Kvalifitseeritud Turvalisuse Hindajat (QSA) või PCI Kohtu-Uurijat (PFI).

Teenusepakkuja Valideerimise Dokumentide Nõuded

Teenusepakkujatel (mitte Kaupmeestel) on kaks võimalikku Taseme klassifikatsiooni. Pärast Teenusepakkuja Taseme määramist [Tabel A-1: Kaupmehe ja Teenusepakkuja Tasemed](#) alusel (eespool), vt [Tabel A-3: Teenusepakkuja Valideerimise Dokumentid](#), et selgitada välja dokumentatsiooni nõuded.

Teenusepakkujaid ei võeta vastu Turbetehnoloogia parandamise programmi.

Tabel A-3: Teenusepakkuja Valideerimise Dokumentid

Tase	Valideerimise Dokumentid	Nõuded
1	Iga-aastane Aruanne Vastavuse Atesteerimise Kohta (ROC AOC)	Kohustuslik
2	Iga-aastane SAQ D (Teenusepakkuja) ja Kvartaalne Võrgustikuanalüüs või Iga-aastane Aruanne Vastavuse Atesteerimise kohta (ROC AOC), kui soovitakse	Kohustuslik

Soovituslik on, et Teenusepakkuja vastaks ühtlasi PCI määratud ettevõtete täiendavale kontrollile.

Turbetehnoloogia Parandamise Programm (STEP)

Kaupmehed, kes vastavad PCI DSSile, võivad American Expressi äranägemisel kvalifitseeruda American Expressi STEPi (Security Technology Enhancement Programme), kui nad võtavad kasutusele teatud täiendavad turbetehnoloogiad oma kaarditöötluskeskkondades. STEP kehtib ainult siis, kui Kaupmees pole viimase 12 kuu jooksul puutunud kokku Andmeintsidendiga ja kui 75% kõigist Kaupmehe Kaarditehingutest on tehtud järgmiste parandatud turbelahenduste kombinatsioonis:

- **EMV, Kontaktivaba EMV või Digitaalne Rahakott (Digital Wallet)** – aktiivsel Kiibipõhisel Seadmel, millel on kehtiv ja ajakohane EMVCo (www.emvco.com) heakskiit/sertifikaat ning mis on võimeline töötleva AEIPSile vastavaid Kiipkaardi Tehinguid. (USA Kaupmehed peavad lisama Kontaktivaba)
- **Kakspunktkrüpteerimist (Point-to-Point Encryption, P2PE)** – edastamine Kaupmehe töötlejale toimub, kasutades PCI-SSC heakskiidetud või QSA heakskiidetud Kakspunkt-krüpteerimissüsteemi
- **Tokeniseeritud** – rakendatav tokeniseerimislahendus peab:
 - vastama EMVCo spetsifikatsioonidele,
 - olema turvatud, töödeldud, talletatud, edastatud ja hallatud terviklikult PCI-le vastava kolmandast osapoolest teenusepakkuja poolt, ning
 - tokenit ei tohi olla võimalik ümber pöörata, et avaldada maskeerimata Esmased Kontonumbrid (PANid) Kaupmehele.

Turbetehnoloogia Parandamise Programmi tingimustele vastavate Kaupmeeste suhtes kehtivad vähendanud PCI Valideerimise Dokumentide nõuded, mida on täpsemalt kirjeldatud jaotises [Meede 3: "Täitke Valideerimise Dokumentid, mille peate saatma American Expressile"](#) allpool.

Meede 3: Täitke Valideerimise Dokumentid, mille peate saatma American Expressile

Järgmised dokumendid on nõutavad erinevate Kaupmehe ja Teenusepakkuja erinevate tasemete jaoks, nagu loetletud tabelites [Tabel A-2: Kaupmehe Valideerimise Dokumentid](#) ja [Tabel A-3: Teenusepakkuja Valideerimise Dokumentid](#) eespool.

Te peate esitama vastavale hindamistüübile sobiva Vastavuse Atesteerimise (AOC). AOC on teie Vastavuse Kinnitus ja selle peab allkirjastama ja sellele lisama kuupäeva teie ettevõtte juhtkonna asjakohane tase.

Lisaks AOC-le võib American Express paluda teil esitada kogu analüüsi koopia ja paluda omal äranägemisel täiendavaid tugidokumente, mis tõendaksid vastavust PCI DSSi nõuetele. See Valideerimise Dokument koostatakse teie kulul.

Vastavuse Atesteerimise Aruanne (ROC AOC) - (iga-aastane nõue) – Aruanne teie seadmete, süsteemide ja võrgustike (ja nende komponentide), kus Kaardiomaniku Andmeid või Tundlikke Autentimise Andmeid (või mõlemaid) talletatakse, töödeldakse või edastatakse, kohapealse üksikasjaliku kontrollimise tulemuste Vastavusdokumentide kohta. On olemas kaks versiooni: üks Kaupmeestele ja teine Teenusepakkujatele. Vastavusaruande peab tegema:

- QSA või
- Ettevõttesisene Turvahindaja (ISA) ja atesteerima teie tegevjuht, finantsjuht, infoturbe juht või direktor

ROCAOC tuleb allkirjastada ja lisada kuupäev QSA või ISA poolt ning juhtkonna volitatud taseme poolt teie ettevõttes ning esitada American Expressile vähemalt korra aastas.

Vastavuse Atesteerimise Eneseanalüüsi Küsimustik (SAQ AOC) - (iga-aastane nõue) – Eneseanalüüsi Küsimustik võimaldab analüüsida ise oma seadmeid, süsteeme ja võrgustikke (ja nende komponente), kus Kaardiomaniku Andmeid või Tundlikke Autentimise Andmeid (või mõlemaid) talletatakse, töödeldakse või edastatakse. SAQst on mitu versiooni. Te valite ühe või enam vastavalt oma Kaardiomaniku Andmete Keskkonnale.

SAQi võib täita teie ettevõtte personal, kes on võimeline küsimustele täpselt ja põhjalikult vastama, või võite paluda ka QSA abi. SAQ AOC peab allkirjastama ja lisama kuupäeva juhtkonna volitatud tase teie ettevõttes ning esitama American Expressile vähemalt korra aastas.

Heakskiidetud Analüüsipakkuja, Väline Võrgustiku Haavatavuse Analüüsi Kokkuvõte (ASV Analüüs) - (90 päeva nõue) – Väline Haavatavuse Analüüs on kaugtest, mis aitab tuvastada võimalikke nõrku külgi, haavatavaid kohti ja teie Kaardiomaniku Andmete Keskkonna välisvõrguga suhtlevate komponentide (nt veebilehed, rakendused, veebiserverid, meiliserverid, avalikkusega suhtlevad domeenid või hostid) vale konfiguratsiooni.

ASV Analüüsi peab tegema Heakskiidetud Analüüsipakkuja (Approved Scanning Vendor, ASV).

Kui SAQ seda nõuab, tuleb ASV Analüüsiaruanne Vastavusanalüüsi Atesteerimise (AOSC) kohta või kommenteeritud kokkuvõtte koos analüüsitud eesmärkide hulga, sertifikaat, mille tulemused vastavad PCI DSSi analüüsiprotseduuridele, ja ASV koostatud vastavusolek esitada American Expressile vähemalt korra 90 päeva järel.

ROC AOC või STEP pole AOSC või ASV analüüsi kommenteeritud kokkuvõtte esitamiseks vajalikud, kui seda pole eraldi nõutud. Kahtluse vältimiseks on Analüüsid kohustuslikud, kui seda nõuatakse kohalduva SAQ-ga.

STEPi Atesteerimise Valideerimise Dokumendid (STEP) - (iga-aastane nõue) – STEP on saadaval ainult Kaupmeestele, kes vastavad eespool toodud jaotise [Meede 2: "Teadke oma Kaupmehe/Teenusepakkuja Taset ja Valideerimise Dokumentide Nõudeid"](#) loetletule. Kui teie ettevõtte kvalifitseerub, peate täitma ja esitama STEPi Atesteerimisvormi American Expressile korra aastas. Iga-aastane STEP atesteerimise vorm on saadaval allalaadimiseks [Portaalis](#). Samuti võite ühendust võtta oma kliendihalduriga või kirjutada e-posti aadressil AXPPCIComplianceProgram@aexp.com.

Mittevastavus PCI DSS nõuetele - (iga-aastane, 90 päeva ja/või ad hoc nõue) – kui te ei vasta PCI DSS nõuetele, siis peate esitama PCI prioriteetse lähenemise tööriista (PAT) kokkuvõtte (saadaval allalaadimiseks PCI Andmeturbe standardite nõukogu veebisaidil).

PAT kokkuvõttele peab olema määratud parandamise kuupäev, mis ei tohi vastavuse saamiseks ületada kahteteist (12) kuud pärast dokumendi täitmise kuupäeva. Te peate American Expressile esitama korrapäraseid uuendusi oma edusammude kohta parandamise suunas Mittevastava Staatuse alusel (1., 2., 3. ja 4. Taseme Kaupmehed; kõik Teenusepakkujad). Vajalikud parandamismeetmed, et saavutada vastavus PCI DSSile, tuleb täita teie kulul.

American Express ei määra mittevastavustasu enne parandamise kuupäeva. Vastavalt [Tabel A-4: Mittevastavustasu](#), vastutate American Expressi ees kõikide hüvitamiskohustuste ees Andmeidentsidentide korral ja kõikide käesoleva poliitika muude sätete täitmise eest.

American Express jätab endale õiguse määrata omal äranägemisel mittevastavustasu kui:

- PCI prioriteetse lähenemise malli pole esitatud vastavalt käesolevas jaotises sätestatud nõuetele,

- PCI prioriteetse lähenemise mallis kirjeldatud mittevastavuse oleku parandismeetmeid pole rakendatud,
- mittevastavuse oleku PCI prioriteetse lähenemise malli mis tahes nõudeid pole täidetud, või
- kohustuslikud vastavuse dokumendid pole esitatud American Expressile vastavaks tähtjaks või nõudmise korral.

Kaupmeestele/Teenusepakkujatele, kes ei vasta nõuetele, mis on kirjeldatud jaotises [Meede 2: Teadke oma Kaupmehe/Teenusepakkuja Taset ja Valideerimise Dokumentide Nõudeid](#), võidakse kohaldada tasu, nagu sätestatud jaotises [Meede 4: Saatke Valideerimise Dokumendid American Expressile](#).

Igasuguse kahtluse vältimiseks: Kaupmehed, kes ei ole PCI DSS-i nõuetega vastavuses, ei ole STEP jaoks sobivad.

Meede 4: Saatke Valideerimise Dokumendid American Expressile

Kõik Kaupmehed ja Teenusepakkujad, kes peavad osalema programmis, peavad esitama Valideerimise Dokumendi tähisega "kohustuslik", nagu on märgitud tabelis jaotises [Meede 2: "Teadke oma Kaupmehe/Teenusepakkuja Taset ja Valideerimise Dokumentide Nõudeid"](#) American Expressile vastavaks tähtjaks.

Te peate esitama oma Valideerimise Dokumendid American Expressile [Portaali](#) kaudu, mille kasutamise tagab teile American Expressi valitud Programmiadministraator. Valideerimise Dokumentide esitamisega te kinnitate ja garanteerite American Expressile, et järgnevalt kirjeldatu vastab tõele (teie parimate oskuste juures):

- Teie hinnang oli täielik ja põhjalik;
- PCI DSS olek on esitamise ajahetkel täpselt esitatud, olgu vastavuse atesteerimise (AOC) või PCI prioriteetse lähenemise tööriista (PAT) kokkuvõtte esitamisel mittevastavuse kohta;
- Te olete volitatud avaldama selles olevat teavet ja esitate Valideerimise Dokumendid American Expressile rikkumata ühegi osapoole õigusi.

Mittevastavustasud ja Lepingu lõpetamine

American Expressil on õigus teile määrata Mittevastavustasusid ja lõpetada Leping, kui te käesolevaid nõudeid ei täida või ei esita American Expressile ette antud tähtajaks kohustuslikke Valideerimise Dokumente. American Express püüab teatada andmeturbe kontaktisikule vastava tähtaja nii iga-aastase kui ka kvartaalse aruandeperioodi kohta.

Tabel A-4: Mittevastavustasu

Kirjeldus*	1. taseme Kaupmees või Teenusepakkuja	2. taseme Kaupmees või Teenusepakkuja	3. taseme või 4. taseme Kaupmees
Mittevastavustasu määratakse, kui Valideerimise Dokumente ei saada esimeseks tähtajaks.	USD 25 000	USD 5000	USD 50
Täiendav mittevastavustasu määratakse, kui valideerimise dokumente ei saada teiseks tähtajaks.	USD 35 000	USD 10 000	USD 100
Täiendav mittevastavustasu määratakse, kui valideerimise dokumente ei saada kolmandaks tähtajaks. MÄRKUS: mittevastavustasu kohaldatakse, kuni valideerimise dokumendid on esitatud.	USD 45 000	USD 15 000	USD 250

* Mittevastavustasud arvestatakse kohaliku valuuta ekvivalentides.

* Ei ole kohaldatav Argentinas.

Kui teie PCI DSS vastavuse dokumentide kohustusi ei täideta, on American Expressil õigus määrata selleks ajaks kogunenud mittevastavustasud, pidada kinni makseid ja/või lõpetada Leping.

Peatükk 3

Andmeintsidentide Haldamise Kohustused

Te peate American Expressi teavitama viivitamatult, kuid mitte hiljem kui seitsmekümne kahe (72) tunni jooksul, alates andmeintsidendi avastamisest.

American Expressi teavitamiseks võtke ühendust American Expressi Ettevõtte Intsidendide Reageerimisprogrammiga (EIRP) tasuta numbril 1.888.732.3750 või 1.602.537.3021, või e-posti aadressil EIRP@aexp.com. Seoses Andmeintsidendiga on teil kohustus määrata endale kontaktisik. Lisaks sellele:

- Te peate läbi viima iga Andmeintsidendi puhul põhjaliku kohtuekspertiisi ja esitama American Expressile koheselt kõik Kompromiteeritud Kaardinumbrid. American Express jätab endale õiguse läbi viia oma enda siseanalüüs, tuvastamaks Andmeintsidendiga seonduvaid andmeid.

Andmeintsidentide puhul, mis on seotud alla 10 000 kordumatu Kaardinumbriga, tuleb American Expressile esitada uurimise kokkuvõtte kümne (10) tööpäeva jooksul pärast uurimise lõpuleviimist.

- Uurimise kokkuvõtte peab sisaldama järgmiseid andmeid: intsidendi kokkuvõtte, mõjutatud keskkonna/keskkondade kirjeldus, sündmuste ajaskaala, olulised kuupäevad, mõju ja seotud andmete üksikasjad, piiramise ja parandamise meetmed ning hinnang selle kohta, et American Expressi andmed pole ohus.

Selliste Andmeintsidentide puhul, mis hõlmavad 10 000 või enamat unikaalset Kaardinumbrit, peate selle uurimise läbiviimiseks viie (5) päeva jooksul pärast andmeintsidendi avastamist kaasama PCI PFI.

- Kohtuekspertiisi muutmata aruanne tuleb pärast selle valmimist edastada American Expressile kümne (10) tööpäeva jooksul.
- Kohtu-uuringu aruanne tuleb koostada, kasutades kehtivat Kohtuekspertiisi Juhtumi Lõpliku Aruande Malli. Kohtu-uuringu aruanne peab sisaldama kohtulikku läbivaatamist, vastavusaruandeid ja kogu teavet, mis on Andmeintsidendiga seotud; välja selgitama Andmeintsidendi põhjuse; kinnitama, kas te olite PCI DSS-iga Andmeintsidendi ajal vastavuses; ja kinnitama oma võimet vältida tulevasi Andmeintsidente, (i) edastades plaani, mille alusel parandada kõik PCI DSS-iga seotud puudujäägid, ja (ii) osaledes American Expressi vastavusprogrammis (nagu allpool kirjeldatud). American Expressi nõudmisel peate te Kvalifitseeritud Turvalisuse Hindaja (Qualified Security Assessor, QSA) kaudu andma kinnituse, et puudujäägid on kõrvaldatud.

Olenemata [Peatükk 3. "Andmeintsidentide Haldamise Kohustused"](#):

- American Express võib omal äranägemisel nõuda PFI kaastamist Andmeintsidendi uurimise läbiviimiseks, mis on seotud alla 10 000 kordumatu Kaardinumbriga või kui 12-kuu jooksul on aset leidnud mitmed intsendid. Selline uurimine peab vastama [Peatükk 3. "Andmeintsidentide Haldamise Kohustused"](#), eelnevalt nimetatud nõuetele ja see tuleb lõpule viia American Expressi poolt nõutud ajavahemikus.
- American Express võib oma äranägemise järgi eraldi kaasata PFI, et läbi viia uuring ükskõik millise Andmeintsidendi kohta ja võib teilt nõuda sellise uuringu kulu katmist.

Te peate hindama Andmeintsidenti, rakendades kohalduvaid andmetega seotud rikkumisest teavitamise seadusi üldiselt ja vajaduse korral, teatama vastavatele regulatiivasutustele ja Kaardi kasutajatele, järgides kohalduvaid andmetega seotud rikkumistest teavitamise seadusi. Kui olete kindlaks teinud, et teie Teenusepakkuja või muu üksus on kohustatud teatama Andmeintsidendist, peate juhtima selle Teenusepakkuja või üksuse tähelepanu sellele, et ta peab täitma oma teavitamise kohustust, vastavalt kohalduvatele andmetega seotud rikkumisest teavitamise seadustele. Te nõustute hankima American Expressi kirjaliku loa enne American Expressile viitamist või American Expressi nimetamist mis tahes suhtluses Kaardi Kasutajatega seoses Andmeintsidendiga. Te peate tegema American Expressiga koostööd, et esitada andmeid ja parandada mistahes vead, mis Andmeintsidendiga seoses ilmnevad, sealhulgas pidama American Expressiga nõu oma (ning hankima vajalikud loobumised andmaks) American Expressile kogu asjakohase teabema edasise suhtluse osas American Expressi Kaardiomanikega, kes on Andmeintsidendist mõjutatud, ja and, kinnitamaks oma võimet vältida tulevasi Andmeintsidente viisil, mis on kooskõlas Lepinguga.

Olenemata mistahes Lepingus olevast vastupidisest konfidentsiaalsuskohustusest, on American Expressil õigus mistahes Andmeintsidendi kohta avalikustada teavet: American Expressi Kaardi Kasutajatele, kaardi väljastajatele, teistele American Expressi võrgu kasutajatele ja üldsusele, nagu seda on kohaldatava õiguse kohaselt nõutud; kohtu-, haldus- või regulatiivse määruse, käskkirja, kohtukutse, nõude või muul alusel selleks, et vähendada pettuse või kahju tekkimise riski või avalikustada mistahes muul viisil, kui see on asjakohane, et hallata American Expressi võrku.

Mida teha, kui teil on aset leidnud Andmeintsident?

Palun järgige neid samme, kui olete oma ettevõttes tuvastanud Andmeintsidendi.



Samm 1:

Täitke [Kaupmeeste Andmeintsidendi esialgse teatise vorm](#) ja saatke see 72 tunni jooksul pärast Andmeintsidendi avastamist e-posti teel aadressile EIRP@aexp.com.



Samm 2:

Viige läbi põhjalik uurimine; see võib teilt nõuda [maksekaarditööstuse \(Payment Card Industry, PCI\) Kohtu-Uurija palkamist](#).



Samm 3:

Esitage meile koheselt kõik kompromiteeritud American Express®-i Kaardi numbrid.



Samm 4:

Tehke meiega koostööd, et aidata lahendada Andmeintsidendi tõttu esile kerkivaid probleeme.

Vaadake [Peatükk 3, "Andmeintsidentide Haldamise Kohustused"](#), et saada üksikasjalikumat teavet Andmeintsidentide haldamise kohustuste kohta.

Kas teil on veel küsimusi?

US: (888) 732 3750 (tasuta)

Rahvusvaheline: +1 (602) 537 3021

EIRP@aexp.com

Peatükk 4

Hüvitamiskohustused Andmeintsidendi Korral

Teie Lepingust tulenevad hüvitamiskohustused American Expressile Andmeintsidentide korral määratakse kindlaks käesoleva jaotise [Peatükk 4, "Hüvitamiskohustused Andmeintsidendi Korral"](#), alusel ilma, et American Express loobuks seejuures teistest õigustest ja õiguskaitsevahenditest. Lisaks teie hüvitamiskohustustele (olemasolu korral), võidakse teile kohaldada Andmeintsidendi mittevastavustasu, nagu kirjeldatud allpool jaotises [Peatükk 4, "Hüvitamiskohustused Andmeintsidendi Korral"](#).

Kompenseerite American Expressile määras, mis on 5 USA dollarit ühe kontonumbri kohta, Andmeintsidendid, mis on seotud:

- 10 000 või rohkem American Expressi Kaardinumbrit ühega järgnevatest:
 - Tundlikud Autentimise Andmed või
 - Kehtivusaja kõpp

Sellegipoolest ei nõua American Express teilt kahjutasu Andmeintsidendi eest, mis hõlmab:

- alla 10 000 American Expressi Kaardinumbrit või
- üle 10 000 American Expressi Kaardinumbri, kui te vastate järgmistele tingimustele:
 - olete teavitanud American Expressi Andmeintsidendist, vastavalt jaotisele [Peatükk 3, "Andmeintsidentide Haldamise Kohustused"](#),
 - te olite Andmeintsidendi ajal vastavuses PCI DSS-iga (nagu see on kindlaks määratud andmeintsidendi PFI juurdlusega), ja
 - Andmeintsident ei olnud põhjustatud teie või teie Seotud Poolte õigusvastasest tegevusest.

Vaatamata [Peatükk 4, "Hüvitamiskohustused Andmeintsidendi Korral"](#), eelnevatele lõikudele olete te kohustatud kompenseerima olenemata American Expressi Kaardi kontonumbrite arvust American Expressile

Andmeintsidendi mittevastavustasu, mis ei ületa 100 000 USA dollarit ühe Andmeintsidendi kohta (American Expressi poolt kindlaks määratud oma äranägemise järgi) juhul, kui te ei järgi teile [Peatükk 3. "Andmeintsidendi Haldamise Kohustused"](#). Kahtluse vältimiseks ei ületa Andmeintsidendi mittevastavustasu kogumaksumus üksiku Andmeintsidendi kohta 100 000 USA dollarit.

American Express jätab oma arvutustest välja kõik American Expressi Kaardi Kontonumbrid, mis olid seotud varem esitatud andmeintsidendi hüvitisnõudega kaheteistkümne (12) kuu jooksul enne Teavitamise Kuupäeva. Kõik American Expressi sel viisil tehtud arvutused on lõplikud.

American Express võib teile esitada Andmeintsidendi mittevastavustasu arve täies ulatuses või arvata summa maha teile määratud American Expressi maksetest (või vastavalt debiteerida teie pangavarvet) kooskõlas Lepinguga.

Teie hüvitamiskohustusi Andmeintsidendi korral ei käsitleta siinkohal juhuslike, kaudsete, spekulatiivsete, tegevusest tulenevate, eriliste või karistuseks või hoiatuseks määratud kahjuhüvitistena Lepinguga alusel. Seda tingimusel, et sellised kohustused ei sisalda kahjuhüvitisi, mis on seotud või mis tulenevad kasumi või tulu kaotusest, maineväärtuse vähenemisest või ärivõimaluste kadumisest.

American Express võib oma äranägemise järgi vähendada Kaupmeeste hüvitamiskohustust üksnes andmeintsidendi puhul, mis vastavad kõigile järgmistele kriteeriumidele:

- asjakohaseid Riski Vähendavaid Tehnoloogiaid kasutati enne Andmeintsidendi ja need olid kasutusel kogu Andmeintsidendi Sündmuse ajal,
- viidi lõpule põhjalik uurimine kooskõlas maksekaarditööstuse andmeturbestandardi kohtu-uurija (PFI) programmiga (välja arvatud juhul, kui eelnevalt ei olnud kirjalikult teisiti kokku lepitud),
- kohtuekspertiisi aruanne toob selgelt välja Riski Vähendavaid Tehnoloogiaid, mida kasutati Andmeintsidendi ajal andmete töötlemisel, säilitamisel ja/või edastamisel, ja
- te ei säilita (ega ole säilitanud kogu Andmeintsidendi Sündmuse ajal) Tundlikke Autentimise Andmeid või mistahes Kaardiomaniku Andmeid, mis ei olnud loetamatuks muudetud.

Kui hüvitise vähendamine on võimalik, määratakse teie hüvitamiskohustuse vähendamine (välja arvatud maksmisele kuuluvad mittevastavustasud) järgmiselt:

Tabel A-5: Hüvitamiskohustuse vähendamise kriteeriumid

Hüvitamiskohustuse vähendamine	Nõutud kriteeriumid
Standardne vähendamine: 50%	> 75% kõikidest Tehingutest on töödeldud Kiibipõhistes Seadmetes ¹ VÕI Riski vähendav Tehnoloogia on kasutusel > 75% Kaupmehe asukohtades ²
Suurendatud määras vähendamine: 75% kuni 100%	> 75% kõikidest Tehingutest on töödeldud Kiibipõhistes Seadmetes ¹ JA muu Riski Vähendav Tehnoloogia on kasutusel > 75% Kaupmehe asukohtades ²

¹ Vastavalt American Expressi siseanalüüsile

² Vastavalt PFI juurdlusele

- Suurendatud määras vähendamine (75% kuni 100%) määratakse kindlaks väikseimalt Tehingu protsendilt, kasutades Kiibipõhiseid Seadmeid JA Kaupmehe asukohti, kus on kasutusel muud Riski Vähendavaid Tehnoloogiaid. Näited [Tabel A-6: Hüvitamiskohustuse suurendatud määras vähendamine](#) näitlikustavad hüvitamiskohustuse vähendamise arvutusi.
- Et kvalifitseeruda Riski Vähendava Tehnoloogiaga, peate te demonstreerima tehnoloogia efektiivset kasutamist kooskõlas selle kujunduse ja sihtotstarbega.
- PFI juurdlus määrab kindlaks Riski Vähendavat Tehnoloogiat kasutavate asukohtade protsendi.

- Hüvitamiskohustuse vähendamine ei rakendu seoses Andmeitsidendiga makstavatele mistahes mittevastavustasudele.

Tabel A-6: Hüvitamiskohustuse suurendatud määras vähendamine

V.a	Kasutatavad Riski Vähendavad Tehnoloogiad	Sobivad	Vähendamine
1	80% Tehingutest Kiibipõhistel Seadmetel 0% asukohtadest kasutab muud Riski Vähendavat Tehnoloogiat	Ei	50%: Standardne vähendamine (vähem kui 75% Riski Vähendava Tehnoloogia kasutamine ei kvalifitseeru suurendatud määras vähendamisenä) ¹
2	80% Tehingutest Kiibipõhistel Seadmetel 77% asukohtadest kasutab muud Riski Vähendavat Tehnoloogiat	Jah	77%: Suurendatud määras vähendamine (põhineb 77% Riski vähendava Tehnoloogia Kasutamisel)
3	93% Tehingutest Kiibipõhistel Seadmetel 100% asukohtadest kasutab muud Riski Vähendavat Tehnoloogiat	Jah	93%: Suurendatud määras vähendamine (põhineb 93% Tehingutel, mis toimuvad Kiibipõhistel Seadmetel)
4	40% Tehingutest Kiibipõhistel Seadmetel 90% asukohtadest kasutab muud Riski Vähendavat Tehnoloogiat	Ei	50%: Standardne vähendamine (vähem kui 75% Tehingutest Kiibipõhistel Seadmetel ei kvalifitseeru Suurendatud määras vähendamisenä)

¹ Andmeitsidendi korral, mis hõlmab 10 000 American Expressi Kaardi kontot, määras 5,00 USA dollarit ühe kontonumbri kohta (10 000 × 5 USA dollarit = 50 000 USA dollarit), võidakse hüvitamiskohustust vähendada 50% võrra, vähendades Hüvitamiskohustust 50 000 USA dollarilt 25 000 USA dollarile, välja arvatud mistahes mittevastavustasu.

Peatükk 5

Sihtanalüüsi programm (Targeted Analysis Programme, TAP)

Kaardiomaniku Andmete kompromiteerimist võivad põhjustada lüngad teie Kaardiomaniku Andmete Keskkonnas (Cardholder Data Environment, CDE).

Näited Kaardiomaniku Andmete kompromiteerimise kohta hõlmavad muuhulgas järgmist:

- Ühine müügikoht (Common Point of Purchase, CPP):** American Expressi Kaardi Kasutajad on teatanud oma kaardikontodel petturlikest tehingutest, ning on tuvastatud ja kindlaks määratud, et need pärinevad ostude tegemisest teie Asutustes.
- Kaardi Andmed leitud:** American Expressi Kaardi ja Kaardiomaniku Andmeid on leitud veebis, seotuna teie Asutustes tehtud Tehingutega.
- Pahavara kahtlus:** American Express kahtlustab, et te kasutate tarkvara, mis on nakatunud ründekoodiga või mis on ründekoodi suhtes haavatav.

TAP on loodud võimalike Kaardiomaniku Andmete kompromiteerimiste identifitseerimiseks.

Teie ja teie Seotud Pooled peate vastama järgmistele nõuetele American Expressi poolse teavituse korral võimalikust Kaardiomaniku Andmete kompromiteerimisest.

- Te peate viivitamatult üle vaatama oma CDE andmeturbe lünkade suhtes ja probleemid parandama.

- Teie kolmandatest osapooltest müüja(d) peavad läbi viima teie CDE põhjaliku uurimise, kui tegemist on tegevuse edasiandmisega.
- Teavituse korral American Expressilt peate te esitama läbiviidud või plaanitud tegevuste kokkuvõtte ülevaatus, hindamise ja/või paranduste kohta.
- Te peate esitama uuendatud PCI DSS valideerimisdokumendid vastavalt [Peatükk 2, "PCI DSS Vastavusprogramm \(teie Süsteemide Oluline Perioodiline Valideerimine\)"](#).
- Kohaldatavuse korral peate te kaasama kvalifitseeritud PCI PFI, kui teie või teie Seotud Pooled:
 - Ei suuda mõistliku aja jooksul lahendada Kaardiomaniku Andmete kompromiteerimist, nagu on kindlaks määratud American Expressi poolt, või
 - kinnitate, et aset on leidnud Andmeidentsident ja vastate [Peatükk 3, "Andmeidentsidentide Haldamise Kohustused"](#) nõuetele.

Tabel A-7: TAP Mittevastavustasu

Kirjeldus	1. taseme Kaupmees või Teenusepakkuja	2. taseme Kaupmees või Teenusepakkuja	3. taseme või 4. taseme Kaupmees
Mittevastavustasu võidakse määrata, kui TAP-iga seotud kohustusi ei täideta esimeseks tähtajaks.	USD 25 000	USD 5000	USD 1000
Mittevastavustasu võidakse määrata, kui TAP-iga seotud kohustusi ei täideta teiseks tähtajaks.	USD 35 000	USD 10 000	USD 2500
Mittevastavustasu võidakse määrata, kui TAP-iga seotud kohustusi ei täideta kolmandaks tähtajaks. MÄRKUS: mittevastavustasusid võidakse määrata, kuni kohustused on täidetud või TAP on lahendatud.	USD 45 000	USD 15 000	USD 5000

Kui teie TAPga seotud kohustusi ei täideta, on American Expressil õigus määrata selleks ajaks kogunenud Mittevastavustasud, pidada kinni makseid ja/või lõpetada Leping.

Peatükk 6

Konfidentsiaalsus

American Express võtab kasutusele sobivad meetmed, et hoida (ja tagada, et tema agendid ja alltöövõtjad, sealhulgas Portaali pakkuja, hoiaksid) teie vastavusaruanded, sealhulgas Valideerimise Dokumendid, konfidentsiaalsetena ja mitte avalikustada Valideerimise Dokumente ühelegi kolmandale osapoolele (muudele kui American Expressi sidusettevõtetele, agentidele, esindajatele, Teenusepakkujatele ja alltöövõtjatele) kolme aasta vältel alates nende kättesaamise kuupäevast. Käesolev konfidentsiaalsuskohustus ei rakendu Valideerimise Dokumentidele, mis:

- on American Expressile teada juba enne avalikustamist;
- on avalikkusele kättesaadavad või muutuvad kättesaadavaks viisil, mil American Express ei riku käesolevat peatükki;
- on American Express õiguspäraselt saanud kolmandalt isikult ilma konfidentsiaalsuskohustuseta;
- on iseseisvalt American Expressil välja töötatud; või
- peavad olema avalikustatud kohtuotsuse, ameti- või valitsusasutuse või mistahes seaduse, eeskirja, määruse, kohtukutse, tuvastamistootluse või muu haldus- või kohtumenetluse või mistahes ametliku või mitteametliku järelepärimise või juurdluse või mistahes valitsusasutuse või muu organi (sealhulgas mistahes järelevalveasutus, inspektor, uurija või õiguskaitseorgani) korraldusel.

Peatükk 7 Vastutuse piirang

AMERICAN EXPRESS LOOBUB SIINKOHAL KÕIGIST KINNITUSTEST, VASTAVUSTEST JA VASTUTUSTEST, NII OTSESEST, KAUDSEST, SEADUSEST VÕI MUUL VIISIL TULENEVAST, SEOS KÄESOLEVA ANDMETURBE TEGEVUSPOLIITIKA, PCI DSS-I JA EMV KIRJELDUSTEGA NING QSA, ASV VÕI PFI (VÕI MÕNE NENDE) MÄÄRAMISE JA NENDE TEGEMISTEGA, SEALHULGAS MISTAHES VASTAVUSEST KAUBANDUSLIKU KVALITEEDI VÕI SOBIVUSE KOHTA MINGI KINDLA EESMÄRGI JAOKS. AMERICAN EXPRESS KAARDI VÄLJASTAJAD EI OLE SELLE POLIITIKA ALUSEL SOODUSTATUD KOLMANDAD ISIKUD.

Peatükk 8 Sõnastik

Järgmisi mõisteid kasutatakse ainult käesoleva *Andmeturbe Tegevuspoliitika* raames:

1. taseme Kaupmees tähistab Kaupmeest, kellel on 2,5 miljonit või rohkem American Expressi Kaardi Tehingut aastas või mistahes Kaupmeest, keda American Express oma äranägemise järgi määrab 1. tasemesse kuuluvaks.

2. taseme Kaupmees tähistab Kaupmeest, kellel on 50 000 või kuni alla 2,5 miljoni American Expressi Kaardi Tehingut aastas.

3. taseme Kaupmees tähistab Kaupmeest, kellel on 10 000 kuni alla 50 000 American Expressi Kaardi Tehingut aastas.

4. taseme Kaupmees tähistab Kaupmeest, kellel on alla 10 000 American Expressi Kaardi Tehingut aastas.

1. taseme Teenusepakkuja tähistab Teenusepakkuja, kellel on 2,5 miljonit või rohkem American Expressi Kaardi Tehingut aastas või mistahes Teenusepakkuja, keda American Express muul juhul peab 1. tasemesse kuuluvaks.

2. taseme Teenusepakkuja tähistab Teenusepakkuja, kellel on alla 2,5 miljoni American Expressi kaardi Tehingut aastas või mis tahes Teenusepakkuja, keda American Express ei pea 1. tasemele kuuluvaks.

American Expressi Kaart ehk **Kaart** tähendab mistahes kaarti, kontole juurdepääsu seadet või makseseadet või teenust, millel on American Expressi või selle sidusettevõtte nimi, logo, kaubamärk, teenusemärk, ärinimi või mistahes muu intellektuaalomandiga kaitstud kujutis või tähis, mis on väljastatud kaardi kontonumbri või kaardi väljastaja poolt.

Andmeintsidenti Sündmus tähendab sissetungi ajavahemikku (või sarnaselt kindlaksmääratud ajavahemikku), mis on esitatud kohtuekspertiisi lõplikus aruandes (näiteks PFI aruandes), või teadmatuse korral kuni 365 päeva enne meile teada antud Andmete Kompromiteerimise võimalikest Kompromiteeritud Kaardinumbritest teavitamise viimast Teavitamise Kuupäeva.

Andmeintsident on intsident, mis hõlmab American Expressi Krüpteerimisvõtmete ohustamist või kahtlustatud ohustamist või vähemalt ühte American Expressi Kaardi kontonumbrit, kus on:

- autoriseerimata juurdepääs või Krüpteerimisvõtmete kasutamine, Kaardiomaniku Andmed või Tundlikud Autentimise Andmed (või nende kombinatsioon), mis on talletatud, töödeldud või edastatud teie seadmesse, süsteemidesse ja/või võrku (või nende osadesse) või mille kasutamist te volitate, võimaldate või teete kättesaadavaks;
- selliste Krüpteerimisvõtmete, Kaardiomaniku Andmete või Tundlike Autentimise Andmete (või nende kombinatsiooni) kasutamine muul eesmärgil kui Lepinguga kooskõlas; ja/või
- kahtlustatav või kinnitatud kadu, vargus või väärkasutamine mistahes meedia, materjalide, dokumentide või teabe abil, mis sisaldavad selliseid Krüpteerimisvõtmeid, Kaardiomaniku Andmeid või Tundlike Autentimise Andmeid (või nende kombinatsiooni).

EMV Spetsifikatsioonid on need spetsifikatsioonid, mille on välja andnud EMVCo, LLC ning mis on kättesaadavad aadressil www.emvco.com.

EMV Tehing on integraallülitusega kaardi (aeg-ajalt nimetatakse ka IC-kaardiks, kiipkaardiks, smart-kaardiks, EMV-kaardiks või ICC-ks) tehing, mis tehakse IC-kaarti lugevas müügikoha terminalis (POS), millel on kehtiv ja ajakohane EMV-tüüpi kinnitus. EMV-tüüpi kinnitused on kättesaadavad aadressil www.emvco.com.

Enesehindamise Küsimustik (SAQ) on Payment Card Industry Security Standards Council, LLC enesehindamise tööriist, mis on mõeldud selleks, et hinnata ja tõendada vastavust PCI DSS-iga.

Esmasel Kontonumbril (PAN) on tähendus, mis on antud sel hetkel kehtiva PCI DSSi mõistete sõnastikus.

Frantsiisiandja on ettevõtja, kes annab litsentsi isikutele või üksustele (Frantsiisivõtjatele), et müüa tooteid ja/või teenuseid Kaubamärgi alusel või seda kasutades; abistab Frantsiisivõtjaid nende äritegevuses või mõjutab Frantsiisivõtjate töömeetodeid; ja nõuab Frantsiisivõtjate käest makseid.

Frantsiisivõtja on sõltumatule omanikule kuuluv ja sõltumatult juhitud kolmas osapool (kaasa arvatud frantsiisivõtja, litsentsisaaja või haru), välja arvatud Sidusettevõtja, kes on Frantsiisiandja poolt litsentseeritud frantsiisi juhtima ja kes on sõlminud kirjaliku lepingu Frantsiisiandjaga, kusjuures ta on alaliselt välja pannud välitähise, identifitseerudes nähtavalt Frantsiisiandja Märkidega või esineb avalikkuse ees Frantsiisiandja ettevõtete grupi liikmena.

Heakskiidetud Kakspunkt-krüpteerimise (P2PE) lahendus tähendab kas PCI SSC loendisse kuuluvat valideeritud lahendust või valideerimist PCI SSC Kvalifitseeritud Turvalisuse Hindaja P2PE ettevõtte poolt.

Heakskiidetud Skaneerimise Läbiviija (ASV) tähendab Üksust, mille on Payment Card Industry Security Standards Council, LLC kvalifitseerinud, et valideerida kindlate PCI DSS nõuete järgimist, viies läbi Internetipõhiste keskkondade haavatavuse skaneerimist.

Kaardi Väljastaja on ükskõik milline üksus (kaasa arvatud American Express või selle Sidusettevõtte), mis on litsentseeritud American Expressi või American Expressi Sidusettevõtte poolt väljastama Kaarte ja osalema Kaartide väljastamise äris.

Kaardinumber tähendab ainulaadset identifitseerimisnumbrit, mille Väljastaja määrab Kaardile väljastamisel.

Kaardi Kasutaja tähendab klienti, kellele maksekaart on väljastatud, või mis tahes isikut, kellel on kaardi kasutamise õigus.

Kaardiomanik tähendab üksikisikut või üksust (i) kes/mis on sõlminud lepingu, millega luuakse kaardi väljastaja juures Kaardi konto, või (ii) kelle/mille nimi on Kaardil.

Kaardiomaniku Andmed tähendab vähemalt täielikku Esmast Kontonumbrit (PAN) eraldi või täielikku PAN-i pluss järgmised andmed: kaardiomaniku nimi, aegumiskuupäev ja/või teenuse kood. Täiendavaid andmeelemente, mida võidakse edastada või töödelda (kuid mitte salvestada) maksetehingu osana, vt Tundlikud Autentimise Andmed.

Kaardiomaniku Andmete Keskkond (CDE) tähistab isikuid, töölusi ja tehnoloogiat, mis talletavad, töötlevad või edastavad kaardiomaniku andmeid või tundlikke autentimise andmeid.

Kaardi Kasutaja Teave on American Expressi Kaardi Kasutajate ja Kaardi Tehingute kohta käiv teave, sealhulgas nimed, aadressid, kaardi kontonumbrid ja kaardi tunnuskoovid (Card Identification, CID).

Kakspunkt-krüpteerimine (P2PE) tähendab lahendust, mis kaitseb krüptograafiliselt konto andmeid alates punktist, kus Kaupmees maksekaardi vastu võtab, kuni turvalise dekrüpteerimispunktni.

Kaupmees tähistab Kaupmeest ja kõiki tema sidusettevõtjaid, kes võtavad vastu American Expressi Kaarte American Expressi või selle sidusettevõtjatega sõlmitud Lepingu alusel.

Kaupmehe tase märgib määratlust, mille me anname Kaupmeestele seoses nende PCI DSSi Vastavuskinnituse Kohustustega, nagu neid on kirjeldatud [Peatükk 2, "PCI DSS Vastavusprogramm \(teie Süsteemide Oluline Perioodiline Valideerimine\)".](#)

Kiibipõhine seade on müügikohapõhine seade, millel on kehtiv ja ajakohane EMVCo (www.emvco.com) kinnitus/sertifikaat ning mis on võimeline töötleva AEIPS-i nõuetele vastavaid Kiipkaardi Tehinguid.

Kiip on Kaarti integreeritud mikrokiip, mis sisaldab Kaardi Kasutaja ja konto teavet.

Kiipkaart on Kaart, mis sisaldab Kiipi ja võib vajada PIN-koodi, et tuvastada Kaardi Kasutaja isikukuuluvust või Kiibis olevat konto teavet või mõlemat (aeg-ajalt nimetatakse ka meie materjalides seda smart-kaardiks, EMV-kaardiks, ICC-ks või intergraallülitusega kaardiks).

Kohtuekspertiisi Juhtumi Lõpliku Aruande Mall tähendab PCI Turvastandardite Nõukogu veebilehel www.pcisecuritystandards.org olevat malli.

Kompromiteeritud kaardinumber tähendab American Expressi Kaardi kontonumbrit, mis on Andmeitsidendiga seotud.

Konto Andmed koosneb Kaardiomaniku Andmetest ja/või Tundlikest Autentimise Andmetest. Vt Kaardiomaniku Andmed ja Tundlikud Autentimise Andmed.

Krediit on Tasu hulk, mille te Kaardi Kasutajatele tagastate Kaardiga tehtud ostude ja maksete eest.

Krediidiandmed tähendab dokumenti Krediidi kohta, mis vastab meie nõuetele.

Krüpteerimisvõti (American Expressi krüpteerimisvõti) tähendab kõiki võtmeid, mida kasutatakse konto andmete töötlemise, tekitamise, laadimise ja/või kaitsmise käigus. See hõlmab muu hulgas järgmist:

- Peamised Krüpteerimisvõtmed: tsooni üldvõtmed (Zone Master Key, ZMK) ja tsooni PIN-võtmed (Zone Pin Key, ZPK)
- Üldvõtmeid kasutatakse turvalistes krüptograafilistes seadmetes: kohalikud üldvõtmed (Local Master Key, LMK)
- Kaardi turvakoodi võtmed (Card Security Code Key, CSCCK)
- PIN-võtmed: tuletusaluse võtmed (Base Derivation Key, BDK), PIN-koodi krüpteerimisvõtmed (PIN Encryption Key, PEK) ja ZPK-d

Kvalifitseeritud Turvalisuse Hindaja (QSA) on üksus, mille on Payment Card Industry Security Standards Council, LLC kvalifitseerinud, et valideerida PCI DSS-i järgimist.

Leping tähendab Üldtingimusi, Kaupmeeste Eeskirju ning kaasnevaid graafikuid ja näidismaterjale, kollektiivselt (vahel nimetatakse meie materjalides: Kaardi Heakskiitmise Leping).

Maksekaarditööstuse Andmeturbestandard (Payment Card Industry Data Security Standard, PCI DSS) on Maksekaarditööstuse Andmeturbestandard, mis on kättesaadav aadressil www.pcisecuritystandards.org.

Maksekaarditööstuse Turvastandardite Nõukogu (Payment Card Industry Security Standards Council, PCI SSC) Nõuded tähendavad maksekaartide andmete, kaasa arvatud PCI DSS ja PA DSS, turve ja kaitsmisega seotud standardite ja nõuete kogu, kättesaadaval aadressil www.pcisecuritystandards.org.

Müügikoha (POS) Süsteem on teabe töötlussüsteem või seade, sealhulgas automaat, personaalarvuti, elektrooniline kassapaar, kontaktivaba luger või makseseade või protsess, mida kasutavad Kaupmehed, et saada volitusi või koguda Tehingu andmeid või mõlemad.

Ostja Algatatud Makse (BIP) Tehingud tähendab digitaalset makselahendust, mis võimaldab ostjatel kiiresti ja efektiivselt planeerida makseid tarnijatele (seotud ettevõtte kaartidega).

PCI DSS on Maksekaarditööstuse Andmeturbestandard, mis on kättesaadav aadressil www.pcisecuritystandards.org.

PCI Kohtu-Uurija (PFI) on üksus, mille on heaks kiitnud Payment Card Industry Security Standards Council, LLC, et läbi viia Maksekaardiandmete rikkumise või kahjustamise kohtuekspertiis.

PCI Poolt Heakskiidetud tähendab, et PIN-Koodi Sisestamise Seade või Väljamakse Avaldus (või mõlemad) kuvatakse kasutuselevõtu ajal heakskiidetud ettevõtete ja pakujate nimekirjas, mida haldab PCI Security Standards Council, LLC, mis on kättesaadav aadressil www.pcisecuritystandards.org.

PCI PIN-Koodi Turvanõuded on Maksekaarditööstuse PIN-Koodi Turvanõuded, mis on kättesaadavad aadressil www.pcisecuritystandards.org.

PIN-Koodi Sisestamise Seadme tähendus on antud Maksekaarditööstuse PIN-Koodi Tehingu Turvalisuse (PIN Transaction Security, PTS) mõjutuspunkti (Point of Interaction, POI) praeguses Terminisõnastikus, modulaarsed turvanõuded, mis on kättesaadavad aadressil www.pcisecuritystandards.org.

Portaal tähendab aruandlussüsteemi, mida pakub American Expressi valitud American Expressi PCI Programmi Administraator. Kaupmehed ja Teenusepakkujad peavad kasutama portaali PCI Valideerimise Dokumentide esitamiseks American Expressile.

Programm tähendab American Expressi PCI Vastavusprogrammi.

Riski Vähendav Tehnoloogia tähistab tehnoloogialahendusi, mis parandavad American Expressi kohaselt American Expressi Kaardiomanike Andmete ja Tundlike Autentimise Andmete turvalisust. Et kvalifitseeruda Riski Vähendava Tehnoloogiana, peate te demonstreerima tehnoloogia efektiivset kasutamist kooskõlas selle kujunduse ja sihtotstarbega. Näited hõlmavad muu hulgas: EMV-d, Kakspunkt-krüpteerimist ja tokeniseerimist.

Seotud Pooled on mistahes või kõik teie töötajad, agendid, esindajad, alltöövõtjad, Töötledjad, Teenusepakkujad, teie müügikoha terminali (POS) seadmete, süsteemide või makse töötlemise lahenduste pakkujad. Üksused, mis on seitud teie American Expressi Kaupmehe kontoga, ja mistahes muu pool, kellele te võite kooskõlas Lepinguga võimaldada ligipääsu Kaardiomaniku Andmetele või Tundlikele Autentimise Andmetele (või mõlemale).

Sihtanalüüsi Programm tähistab programmi, mis tuvastab varakult võimaliku Kaardiomaniku andmete kompromiteerimise teie Kaardiomaniku Andmete Keskkonnas (CDE). Vt [Peatükk 5. "Sihtanalüüsi programm \(Targeted Analysis Programme, TAP\)"](#).

Skaneerimise Nõuete Vastavuskinnitus (AOSC) tähendab teie vastavusstaatust PCI DSS-iga baseerudes võrgu skaneerimisele, mis on Payment Card Industry Security Standards Council, LLC esitatud tüüpvormis.

Tarbija on määratletud kui kaardiomanik, kes ostab kaupsid, teenuseid või mõlemat.

Tasu on Kaardiga tehtud makse või ost.

Tasuandmed tähendab reprodutseeritavat (nii paberil kui elektroonilist) dokumenti Tasu kohta, mis vastab meie nõuetele ja sisaldab Kaardinumbrit, Tehingu kuupäeva, summat dollarites, Heakskiitmist, Kaardi Kasutaja allkirja (kui kohaldub) ja muud infot.

Teavitamise Kuupäev on kuupäev, millal American Express saabab kaardi väljastajale viimase Andmeintsidendi teavituse. Selline kuupäev sõltub American Expressi lõpliku kohtuaruande või siseanalüüsi saamisest ja kuupäev määratakse kindlaks American Expressi enda äranägemisel.

Teenusepakkujad on volitatud töötledjad, kolmandast isikust töötledjad, juurdepääsu pakkujad, POS-Süsteemi lõimijad ja muud Kaupmeestele POS-Süsteemide pakkujad või muud maksete töötlemise lahendused või teenused.

Tehing tähendab Tasu, Krediiti, Ettemakset (või muud juurdepääsu rahale) või pangaautomaadi tehingut, mis on Kaardi abil tehtud.

Tehingu Andmed tähendab kõiki American Expressi nõutud andmeid ühe või mitme Tehingu tõendamiseks, sealhulgas müügikohus kogutud andmeid, Autoriseerimise ja Edastamise ning võimaliku Tagastamise käigus kogutud või genereeritud andmeid.

Token tähendab krüptograafilist tokenit, mis asendab PANi ennustamatu väärtuse antud indeksi alusel.

Töötledja on Kaupmeestele teenusepakkuja, kes hõlbustab esitatu autoriseerimist ja töötlemist American Expressi võrgus.

Tundlikud Autentimise Andmed tähendab turvalisusega seotud andmeid, mida kasutatakse kaardiomanike autentimiseks ja/või maksekaartide tehingute autoriseerimiseks. See info sisaldab muuhulgas kaardi kinnituskoodi, täielikke jälgimisandmeid (magnetribalt või kiibilt), PIN-koodi ja PIN-plokke.

Turbetehnoloogia Parandamise Programm ehk STEP on American Expressi programm, milles julgustatakse Kaupmehi kasutama tehnoloogiaid, mis parandavad andmeturvet.

Valideerimise Dokumendid on AOC esitatud dokumendid, mis on tehtud koos iga-aastase kohapealse turvalisuse hindamise või SAQ, AOSC ja tulemuste kokkuvõtetega, mis on tehtud seoses iga-kvartalilise võrgu skaneerimisega või iga-aastase Turbetehnoloogia Parandamise Programmi kinnitamisega.

Väljamakse Avaldus omab tähendust, mis on sellele antud Turvalise Tarkvara Standardi ja Turvalise Tarkvara Elutsükli Standardi Terminisõnastikus, kättesaadaval aadressil www.pcisecuritystandards.org.

Vastavuskinnitus (AOC) tähendab teie vastavusstaatust PCI DSS-iga, mis on Payment Card Industry Security Standards Council, LLC esitatud tüüpvormis.

Peatükk 9 Kasulikud veebisaidid

American Expressi Andmeturve: www.americanexpress.com/datasecurity

Maksekaartitööstuse Andmeturbestandardi Nõukogu (PCI Security Standards Council, LLC):
www.pcisecuritystandards.org

EMVCo: www.emvco.com