

Reglur um gagnaöryggi (DSOP)

Kafli 1	Kynning á DSOP og staðlar um vernd	3
Kafli 2	PCI DSS-samræmisáætlun (mikilvæg reglubundin staðfesting á kerfum þínum)	3
Aðgerð 1:	Taktu þátt í Áætlun American Express varðandi hlífingu við þessar Reglur	4
Aðgerð 2:	Hafðu skilning á þínu stigi Söluaðila/Þjónustuveitanda og kröfum um Staðfestingargögn	4
Aðgerð 3:	Kláraðu Staðfestingargögnin sem þú þarft að senda American Express	7
Aðgerð 4:	Staðfestingargögn send til American Express	9
Kafli 3	Stjórnunarskyldur vegna Gagnatilfella	10
Kafli 4	Skaðabótaskyldur vegna Gagnatilfella	12
Kafli 5	Áætlun um miðaða greiningu (TAP)	14
Kafli 6	Þagnarskylda	15
Kafli 7	Fyrirvari	15
Kafli 8	Orðalisti	16
Kafli 9	Gagnleg vefsvæði	19

DSOP Samantekt yfir breytingar

Myndtákn

Mikilvægar uppfærslur eru taldar upp í Samantektartöflu yfir breytingar en þær eru einnig sýndar í *DSOP* með breytingastiku. Breytingastikur eru lóðréttar línur á vinstri spássíu sem gefa til kynna að texti hefur verið endurskoðaður eða bætt hefur verið við hann. Aðeins verulegar breytingar í *DSOP* með mögulegum áhrifum á verklagsreglur Söluaðila eru sýndar með breytingastiku eins og sýnt er á vinstri spássíu.



Fjarlægður texti er auðkenndur með ruslatunnutákni á spássíu við hlið þýðingarmikillar eyðingar á texta, að meðtöldum köflum, töflum, málsgreinum, athugasemdum og punktum. Vísað er til texta sem hefur verið fjarlægður í þessari Samantekt á breytingum með því að nota kaflanúmerið úr fyrri útgáfu til að forðast rugling.

Bláar línur sem liggja meðfram málsgreinum gefa til kynna svæðisbundnar upplýsingar.

Samantektartafla yfir breytingar

Mikilvægar uppfærslur eru taldar upp í eftirfarandi töflu en þær eru einnig sýndar í *DSOP* með breytingastiku.

Kafli/undirkafli	Lýsing á breytingu
Það eru engar breytingar í þessari útgáfu.	

Kafli 1

Kynning á DSOP og staðlar um vernd

Sem leiðandi fyrirtæki í neytendavernd hefur American Express til langs tíma skuldbundið sig til að vernda Korthafaupplýsingar og Viðkvæm auðkenningargögn til að tryggja öryggi þeirra.

Gagnaleki hefur neikvæð áhrif á neytendur, Söluaðila, Þjónustuveitendur og kortaútgefendur. Eitt stakt tilfelli getur valdið alvarlegum skaða á orðspori fyrirtækis og skert getu þess til að stunda viðskipti. Hægt er að auka tiltrú viðskiptavina, afkomu og orðspor fyrirtækis með því að takast á við þessa ógn með innleiðingu öryggisreglna.

American Express veit að Söluaðilar og Þjónustuveitendur okkar (einu nafni kallaðir þú eða þið) deila áhyggjum okkar og fer fram á það af þér, sem hluta af skyldum þínum, að **þú** hlítir gagnaöryggisákvæðunum í Samningi þínum um viðtöku (í tilviki Söluaðila) eða vinnslu (í tilviki Þjónustuveitenda) á American Express® kortinu (báðir nefndir **Samningurinn**) svo og þessum Reglum um gagnaöryggi (DSOP), sem okkur er heimilt að breyta hvenær sem er. Þessar skyldur eiga við um allan búnað, kerfi og netkerfi þín þar sem Dulkóðunarlyklar, Korthafaupplýsingar eða Viðkvæm auðkenningargögn (eða bæði) eru geymd, unnið er úr þeim eða þau send.

Hugtök sem hér eru notuð í hástöfum en eru ekki sérstaklega skilgreind hafa þá merkingu sem þeim er gefin í orðalistanum aftast í þessum reglum.

Reglur um gagnaöryggi (DSOP) er safn yfirgripsmikilla regluskilyrða sem ætluð eru til að vernda reikningsgögn hvenær sem slík gögn eru geymd, unnið er úr þeim eða þau send.

American Express krefur alla Söluaðila og Þjónustuveitendur að hlíta Gagnaöryggisstaðli Greiðslukortafyrirtækja (PCI DSS). Sem hluti af þeirri kröfu ber þér að gera eftirfarandi og sjá til þess að Tilgreindir aðilar þínir geri það líka:

- geyma Korthafaupplýsingar aðeins í því skyni að greiða fyrir viðskipti með American Express-kortinu, í samræmi við ákvæði og skilyrði Samningsins.
- hlíta nýjustu útgáfu Gagnaöryggisstaðals Greiðslukortafyrirtækja (PCI DSS) og öðrum PCI-öryggiskröfum (PCI SSC) vegna vinnslu, geymslu eða sendingu Dulkóðunarlykla, Korthafaupplýsinga eða Viðkvæmra auðkenningargagna eigi síðar en þann dag sem sú útgáfa viðkomandi kröfu tók gildi.
- tryggja að PCI-viðurkenndar vörur séu notaðar þegar tækni er tekin í notkun eða skipt út til að geyma, vinna eða senda gögn.

Þér ber að vernda allar American Express-upplýsingar um Kvittanir og Endurgreiðslufjárhæðir sem haldið er eftir samkvæmt Samningnum í samræmi við þessi gagnaöryggisákvæði. Þú skalt aðeins nota þessar upplýsingar í því skyni að uppfylla skyldur þínar samkvæmt Samningnum og gæta þeirra í samræmi við það. Þú berð fjárhagslega og annarskonar ábyrgð gagnvart American Express á því að tryggja að Tilgreindir aðilar þínir hlíti þessum gagnaöryggisákvæðum (fyrir utan það að sýna að Tilgreindir aðilar þínir hlíti þessum reglum samkvæmt [Kafli 2, „PCI DSS-samræmisáætlun \(mikilvæg reglubundin staðfesting á kerfum þínum\)“](#), nema annað sé kveðið á um í þeim kafla). Upplýsingar um PCI-staðlana og hvernig skal hlíta kröfum þeirra er að finna á www.pcisecuritystandards.org.

Kafli 2

PCI DSS-samræmisáætlun (mikilvæg reglubundin staðfesting á kerfum þínum)

Þér ber að grípa til eftirfarandi aðgerða til að staðfesta, árlega og á 90 daga fresti í samræmi við PCI DSS-staðalinn eins og lýst er að neðan, stöðu búnaðar þíns, kerfa og/eða netkerfa (og íhluta þeirra) sem geyma, vinna úr eða senda Korthafaupplýsingar eða Viðkvæm auðkenningargögn.

Fjórar aðgerðir þarf til að ljúka staðfestingunni:

- [Aðgerð 1](#): Taktu þátt í PCI-Áætlun American Express varðandi hlítingu við þessar reglur.
- [Aðgerð 2](#): Hafðu skilning á þínu stigi Söluaðila/Þjónustuveitenda og kröfum um Staðfestingargögn.
- [Aðgerð 3](#): Kláraðu Staðfestingargögnin sem þú þarft að senda American Express.
- [Aðgerð 4](#): Sendu Staðfestingargögnin til American Express innan fyrirskipaðra tímamarka.

Aðgerð 1: Taktu þátt í Áætlun American Express varðandi hlítingu við þessar Reglur

Stig 1 Söluaðilar, Stig 2 Söluaðilar, og allir þjónustuveitendur, eins og lýst er hér að neðan, verða að taka þátt í Áætluninni samkvæmt þessari stefnu. American Express getur, að eigin vild, tilnefnt sérstaka Stig 3 og Stig 4 Söluaðila til að taka þátt í Áætluninni samkvæmt þessari stefnu.

Söluaðilar og þjónustuveitendur sem þurfa að taka þátt í Áætluninni verða að skrá sig í [Gáttinni](#) sem veitt er af Kerfisstjóranum sem valinn er af American Express innan tilgreindra tímamarka.

- Þú verður að samþykkja alla sanngjarna skilmála og skilyrði sem tengjast notkun Gáttarinnar.
- Þú verður að úthluta og veita nákvæmar upplýsingar fyrir að minnsta kosti einn gagnaöryggistengilið innan Gáttarinnar. Nauðsynlegar upplýsingar innihalda::
 - fullt nafn
 - netfang
 - símanúmer
 - heimilisfang
- Þú verður að veita uppfærðar eða nýjar tengiliðaupplýsingar fyrir gagnaöryggistengiliðinn í Gáttinni þegar upplýsingarnar breytast.
- Þú verður að tryggja að kerfin þín séu uppfærð til að leyfa samskipti úr léni Gáttarinnar.

Verði meinbugir á að veita eða viðhalda núverandi tengiliðaupplýsingum vegna gagnaöryggis eða virkja tölvupóstsamskipti mun það ekki hafa áhrif á rétt okkar til að rukka gjöld.

Aðgerð 2: Hafðu skilning á þínu stigi Söluaðila/Þjónustuveitanda og kröfum um Staðfestingargögn

Hér eru fjögur Stig til notkunar fyrir Söluaðila og tvö stig til notkunar fyrir Þjónustuveitendur sem byggjast á þínum fjölda af American Express-kortafærslum.

- Fyrir Söluaðila þá er magnið sent af Einingum sem sýna flest American Express Söluaðilastig.*
- Fyrir Þjónustuveitendur er þetta summan af magni sem Þjónustuveitan og Þjónustuveita aðila sem þú veitir þjónustu leggja fram.

BIP-færslur (Buyer Initiated Payments) eru ekki innifaldar í magni American Express-kortafærslna til að ákvarða Stig Söluaðila eða staðfestingarkröfur. Þú munt tilheyra einu af Stigum Söluaðila sem tilgreind eru í [Töflu A-1 Stig Söluaðila og Þjónustuveitanda](#).

* Í tilfelli Sérleyfisgjafa þá felur það í sér það magn sem kemur frá fyrirtækjum Sérleyfishafa þeirra. Sérleyfisveitendur sem fyrirskipa Sérleyfishöfum sínum að nota ákveðið Posakerfi (POS) eða Þjónustuveitanda verða einnig að útvega staðfestingargögn fyrir viðkomandi Sérleyfishafa.

Tafla A-1: Stig Söluaðila og Þjónustuveitanda

Stig Söluaðila	Árlegar American Express-færslur
1. stigs Söluaðili	2,5 milljón American Express-kortafærslur eða fleiri á ári, eða hver sá Söluaðili sem American Express útnefnir sem 1. stigs.
2. stigs Söluaðili	50.000 til færri en 2,5 milljón American Express-kortafærslur á ári.
3. stigs Söluaðili	10.000 til færri en 50.000 American Express-kortafærslur á ári.
4. stigs Söluaðili	Færri en 10.000 American Express-kortafærslur á ári.
Stig Þjónustuveitanda	Árlegar American Express-færslur
1. stigs Þjónustuveitandi	2,5 milljón American Express-kortafærslur eða fleiri á ári, eða hver sá Þjónustuveitandi sem American Express telur vera 1. stigs.
2. stigs Þjónustuveitandi	færri en 2,5 milljón American Express-kortafærslur á ári, eða hver sá Þjónustuveitandi sem American Express telur ekki vera 1. stigs.

Skilyrði Söluaðila varðandi Staðfestingargögn

Söluaðilar (ekki Þjónustuveitendur) hafa fjóra mögulega flokka fyrir Stig Söluaðila. Eftir að stig Söluaðila hefur verið ákvarðað með [Töflu A-1 Stig Söluaðila og Þjónustuveitanda](#) (að ofan), má sjá [Töflu A-2 Staðfestingargögn Söluaðila](#) til að ákvarða kröfur um staðfestingargögn.

Tafla A-2: Staðfestingargögn Söluaðila

Stig Söluaðila/ Árlegar American Express-færslur	Skýrsla um Samræmis- vottun Staðfesting um Samræmis- vottun (ROC AOC)	Sjálfsmatsspurningalisti um Samræmisvottun (SAQ AOC) OG Ársfjórðungsleg Ytri Tengiliða Varnarleysisskönnun (Skönnun)	Vottun um Áætlun um aukna öryggistækni (STEP) fyrir gjaldgenga Söluaðila
1. stig/ 2,5 milljónir eða meira	Skylda	Á ekki við	Valkvætt með samþykki American Express (kemur í stað ROC)
2. stig/ 50.000 til færri en 2,5 milljónir	Valkvætt	SAQ AOC skylda (nema lagt sé fram ROC AOC); skönnun er skylda í tengslum við tilteknar gerðir SAQ	Valkvætt með samþykki American Express* (kemur í stað SAQ og netkerfisskönnunar eða ROC)
3. stig**/ 10.000 til færri en 50.000	Valkvætt	SAQ AOC er valkvætt (skylda ef American Express fer fram á það); skönnun er skylda í tengslum við tilteknar gerðir SAQ	Valkvætt með samþykki American Express* (kemur í stað SAQ og netkerfisskönnunar eða ROC)
4. stig**/ Færri en 10.000	Valkvætt	SAQ AOC er valkvætt (skylda ef American Express fer fram á það); skönnun er skylda í tengslum við tilteknar gerðir SAQ	Valkvætt með samþykki American Express* (kemur í stað SAQ og netkerfisskönnunar eða ROC)

* **Athugið:** PCI-teymi American Express mun fara yfir beiðnina og hæfni og staðfesta hvort þú uppfyllir skilyrði fyrir STEP-áætlun. Hafðu samband við þjónustufulltrúann þinn og/eða AXPCComplianceProgram@aexp.com til að athuga hæfni.

**Til að koma í veg fyrir misskilning þá þurfa Söluaðilar af Stigi 3 og Stigi 4 ekki að senda inn Staðfestingargögn nema American Express krefjist þess. Hinsvegar verða þeir að hlíta þessum Reglum um gagnaöryggi og eru skaðabótaskyldir samkvæmt öllum öðrum ákvæðum þeirra.

American Express áskilur sér rétt til að sannreyna sannleiksgildi, nákvæmni, og velsæmi PCI-Staðfestingargagna þinna. American Express gæti krafist þess að þú leggir fram viðbótarskjöl vegna mats til stuðnings þessu markmiði. Að auki hefur American Express rétt á að krefjast þess að þú tileinkir þér PCI-Öryggisstaðlaráðs samþykktan Viðurkenndan úttektaraðila (QSA) eða PCI-rannsóknaraðila (PFI).

Kröfur um Staðfestingargögn Þjónustuveitanda

Þjónustuveitendur (ekki Söluaðilar) eiga tvo flokkunarvalkosti fyrir Stig. Eftir að stig Þjónustuveitanda hefur verið ákvarðað með [Töflu A-1 Stig Söluaðila og Þjónustuveitanda](#) (að ofan), má sjá [Töflu A-3 Staðfestingargögn Þjónustuveitanda](#) til að ákvarða kröfur um staðfestingargögn.

Þjónustuveitendur koma ekki til greina fyrir STEP.

Tafla A-3: Staðfestingargögn Þjónustuveitanda

Stig	Staðfestingargögn	Krafa
1	Árleg Skýrsla um Samræmisvottun Staðfesting um Samræmisvottun (ROC AOC)	Skylda
2	Árleg SAQ D (Þjónustuveitandi) og ársfjórðungsleg netskönnun eða árleg Skýrsla um Samræmisvottun Staðfesting um Samræmisvottun (ROC AOC), ef óskað er eftir	Skylda

Ráðlagt er að Þjónustuveitendur hlíti einnig Viðbótarstaðfestingu PCI-úthlutaðra aðila.

Áætlun um aukna öryggistækni (STEP)

Söluaðilar sem uppfylla PCI DSS-staðalinn geta einnig, að eigin ákvörðun American Express, verið gjaldgengir í áætlun American Express um aukna öryggistækni (STEP) ef þeir innleiða tiltekna aukna öryggistækni í öllu Kortavinnsluumhverfi þeirra. Söluaðilar eru aðeins gjaldgengir í STEP ef þeir hafa ekki orðið fyrir Gagnatilviki síðustu 12 mánuði og ef 75% allra Kortafærslna söluaðila eru framkvæmdar með samblandi af eftirfarandi auknum öryggisvalkostum:

- **EMV, EMV Snertilaust eða Stafrænt Veski** – á virku tæki með gildu EMVCo (www.emvco.com) samþykki/vottun og fært um að vinna úr AEIPS-samhæfðu Flögukortafærslum. (Bandarískir Söluaðilar verða að styðja Snertilausar greiðslur)
- **Dulkóðuð gögn frá punkti til punkts (P2PE)** – send í örgjörva Söluaðila með PCI-SCC-viðurkenndu eða QSA-viðurkenndu Dulkóðunarkerfi frá punkti til punkts
- **Merknuð** – innleidda merkningin verður að:
 - uppfylla skilyrði EMVCo,
 - að vera örugg, unnin, geymd, send og að öllu leyti stjórnað af PCI-samræmdri þjónustuveitu þriðja aðila, og
 - ekki sé hægt að snúa Merkingu til baka þannig að Söluaðilinn geti greint Reikningsnúmerið (PAN).

Kröfur um PCI-Staðfestingargögn eru minni fyrir Söluaðila sem eru gjaldgengir fyrir STEP, eins og nánar er lýst í [Aðgerð 3: „Kláraðu Staðfestingargögnin sem þú þarft að senda American Express“](#) hér fyrir neðan.

Aðgerð 3: Kláraðu Staðfestingargögnin sem þú þarft að senda American Express

Eftirfarandi gagna er krafist fyrir mismunandi stig Söluaðila og Þjónustuveitenda eins og kemur fram í [Töflu A-2 Staðfestingargögn Söluaðila](#) og [Töflu A-3 Staðfestingargögn Þjónustuveitanda](#) hér að ofan.

Þú verður að leggja fram Staðfesting um Samræmisvottun (AOC) fyrir viðeigandi matsgerð. AOC er yfirlýsing um samræmisstöðu þína og verður sem slík að vera undirrituð og dagsett af viðeigandi aðilum innan fyrirtækis þíns.

Til viðbótar við AOC-vottunina getur American Express krafist þess að þú leggir fram afrit af heildarmatinu og ef óskað er eftir viðbótarfylgiskjólum sem sýna fram á samræmi við PCI DSS-kröfur. Þessi Vottun er framkvæmd á þinn kostnað.

Skýrsla um Samræmisvottun Staðfesting um Samræmisvottun (ROC AOC) - (Árleg krafa) – Skýrsla um Samræmingu greinir frá nákvæmri skoðun á búnaði þínum, kerfum og netkerfum (og íhlutum þeirra) þar sem Korthafagögn eða Viðkvæm auðkenningargögn (eða hvoru tveggja) eru geymd, unnin eða send. Það eru tvær

útgáfur: ein fyrir Söluaðila og hin fyrir Þjónustuveitanda. Skýrsla um Samræmisvottun verður að vera framkvæmd af:

- QSA eða
- Innri öryggisaðila (ISA) og staðfest af forstjóra þínum, fjármálastjóra, upplýsingaöryggisstjóra eða yfirmanni

ROC AOC-skýrslan verður að vera undirrituð og dagsett af QSA eða ISA og viðurkenndum leiðtogum innan fyrirtækis þíns og berist til American Express að minnsta kosti einu sinni á ári.

Sjálfsmatsspurningalisti um Samræmisvottun (SAQ AOC) - (Árleg krafa) – Sjálfsmatsspurningalistarnir leyfa sjálfsskoðun á búnaði þínum, kerfum og netkerfum (og íhlutum) þar sem Korthafagögn eða Viðkvæm auðkenningargögn (eða hvoru tveggja) eru geymd, unnin eða send. Það eru margar útgáfur af SAQ. Þú velur eina eða fleiri miðað við Gagnaumhverfi korthafa.

SAQ getur verið fyllt út af starfsfólki innan fyrirtækis þíns sem er hæft til að svara spurningunum með ítarlegum hætti eða þú getur fengið QSA til að aðstoða þig. SAQ AOC-vottunin verður að vera undirrituð og dagsett af til þess bærum stjórnendum innan fyrirtækis þíns og afhent American Express að minnst kosti einu sinni á ári.

Veikleikaskönnun á ytri netkerfum, framkvæmd af samþykktum skönnunaraðila (ASV-Skönnun) - (90 daga krafa) – Ytri veikleikaskönnun er fjartengd til að greina hugsanlega veikleika og rangar stillingar á íhlutum sem snúa að internetinu í Gagnaumhverfi korthafa (t.d. vefsvæði, forrit, vefþjónar, pósthjónar, almenn lén og netveitur).

Hún skal framkvæmd af Viðurkenndum skönnunaraðila (ASV).

Ef SAQ krefst þess verður að senda ASV-Skönnunarskýrslu Vottun um Skönnun Samræmi (AOSC) eða yfirlit, þar á meðal fjöldann sem skannaður var, samræmisvottun um að niðurstöðurnar uppfylli PCI DSS-skönnunarferla og samræmisstöðu sem ASV hefur lokið við, til American Express að minnsta kosti einu sinni á 90 daga fresti.

Ef sent er inn ROC AOC eða STEP þarft þú ekki að leggja fram AOSC eða ASV-skönnunaryfirlit nema þess sé sérstaklega óskað. Til að forðast misskilning þá eru skannanir tilskildar ef þeirra er krafist af SAQ.

STEP Samræm Vottunargögn (STEP) - (Árleg krafa) – STEP er eingöngu í boði fyrir Söluaðila sem uppfylla skilyrði í [Aðgerð 2: „Hafðu skilning á þínu stigi Söluaðila/Þjónustuveitanda og kröfum um Staðfestingargögn“](#) hér að ofan. Ef fyrirtæki þitt uppfyllir skilyrðin verður þú að fylla út og leggja fram STEP-vottunareyðublaðið árlega til American Express. Hægt er að hlaða niður árlega STEP-vottunareyðublaðinu af [Gáttinni](#). Þú getur einnig leitað til þjónustufulltrúa þíns eða skrifað til American Express á AXPPCIComplianceProgram@aexp.com.

Ekki farið eftir PCI DSS - (Árlegt, 90 daga og/eða þegar þess er óskað) – Ef þú ert ekki í samræmi við PCI DSS, þá verður þú að leggja fram yfirlit yfir PCI-forgangsstöðun (PAT) (hægt að hlaða niður í gegnum vefsíðu PCI-öryggisstaðlaráðs).

PAT-yfirlitið verður að tilgreina úrbótadagsetningu, sem má ekki vera lengri en tólf (12) mánuði eftir dagsetningu skjalsins til að ná markmiðum. Þú skalt upplýsa American Express með reglubundnum hætti um framgang úrbóta þinna vegna Misbrests (Stig 1, Stig 2, Stig 3 og Stig 4 Söluaðila; allir Þjónustuveitendur). Aðgerðir til úrbóta sem nauðsynlegar eru til að ná fram samræmi við PCI DSS eiga að vera framkvæmdar á þinn kostnað.

American Express mun ekki leggja á gjöld vegna reglubrota fyrir dagsetningu úrbóta. Samkvæmt [Töflu A-4 Gjald vegna reglubrota](#) ert þú áfram ábyrg(ur) gagnvart American Express fyrir öllum skaðabótaskyldum vegna Gagnatílfella og ert bundin(n) öllum öðrum ákvæðum þessara reglna.

American Express getur að eigin geðþótta haldið réttinum til að leggja á gjöld vegna reglubrota ef:

- sniðmát fyrir PCI-forgangsstöðun hefur ekki verið sent inn í samræmi við kröfurnar sem koma fram í þessum kafla,
- ekki hefur verið farið eftir úrbótaskrefunum fyrir þá stöðu þegar misbrestur er á hlítni sem lýst er í sniðmáttinu fyrir PCI-forgangsstöðun,
- einhverjar kröfur í sniðmáttinu fyrir PCI-forgangsstöðun fyrir þá stöðu þegar misbrestur er á hlítni voru ekki uppfylltar, eða
- tilskilin hlífingargögn voru ekki afhent American Express fyrir gildandi frest eða samkvæmt beiðni.

Söluaðilar/Þjónustuveitendur sem verða ekki við kröfunum í [Aðgerð 2: Hafðu skilning á þínu stigi Söluaðila/Þjónustuveitanda og kröfum um Staðfestingargögn](#), gætu þurft að greiða gjöld sem koma fram í [Aðgerð 4: Staðfestingargögn send til American Express](#).

Til að forðast misskilning þá koma Söluaðilar sem ekki hlíta PCI DSS ekki til greina fyrir STEP.

Aðgerð 4: Staðfestingargögn send til American Express

Allir Söluaðilar og Þjónustuveitendur sem þurfa að taka þátt í Áætluninni verða að leggja fram Staðfestingargögn merkt „skyldubundið“ í töflunum í [Aðgerð 2: „Hafðu skilning á þínu stigi Söluaðila/Þjónustuveitanda og kröfum um Staðfestingargögn“](#) til American Express áður en frestur rennur út.

Þú verður að leggja fram Staðfestingargögnin þín til American Express með því að nota [Gáttina](#) sem kerfisstjórninn sem American Express hefur valið hefur útvegað. Með því að leggja fram Staðfestingargögnin staðfestir þú og ábyrgist við American Express að eftirfarandi sé satt (eftir bestu vitund):

- Matið þitt var útfært að fullu og ítarlegt;
- PCI DSS-staða er nákvæmlega sýnd þegar að henni lauk, hvort sem sent hafi verið inn Staðfesting um Samræmisvottun (AOC) eða PCI-forgangsnálgunartöl fyrir samantekt;
- Þú hefur heimild til að birta upplýsingarnar sem þar er að finna og gefur American Express Staðfestingargögnin án þess að brjóta á rétti annars aðila.

Gjöld vegna reglubrots og uppsögn Samnings

American Express er heimilt að innheimta af þér gjöld vegna reglubrots og segja upp Samningnum ef þú uppfyllir ekki þessar kröfur eða sendir ekki nauðsynleg Staðfestingargögn til American Express áður en skilafrestur rennur út. American Express mun reyna að láta gagnaöryggistengilið vita hver viðeigandi skilafrestur er fyrir hvert árlegt og ársfjórðungslegt skýrslutímabil.

Tafla A-4: Gjald vegna reglubrota

Lýsing*	Söluaðili á 1. stigi eða Þjónustuveitandi á 1. stigi	Söluaðili á 2. stigi eða Þjónustuveitandi á 2. stigi	Söluaðili á 3. stigi eða 4. stigi
Gjald vegna reglubrots verður lagt á ef Staðfestingargögn berast ekki fyrir fyrsta skilafrest.	25.000\$ Bandaríkjadallir	5.000\$ Bandaríkjadallir	50\$ Bandaríkjadallir
Viðbótargjald vegna reglubrots verður lagt á ef Staðfestingargögn berast ekki fyrir annan skilafrest.	35.000\$ Bandaríkjadallir	10.000\$ Bandaríkjadallir	100\$ Bandaríkjadallir
Viðbótargjald vegna reglubrots verður lagt á ef Staðfestingargögn berast ekki fyrir þriðja skilafrest. ATHUGIÐ: Gjöld vegna reglubrots verða áfram notuð þar til Staðfestingargögnin eru komin í hús.	45.000\$ Bandaríkjadallir	15.000\$ Bandaríkjadallir	250\$ Bandaríkjadallir

*Gjöld vegna reglubrots eru lögð á í Staðbundnum gjaldmiðli.

* Á ekki við í Argentínu.

Ef PCI DSS-hlífingargögn þín uppfylla ekki kröfur þá hefur American Express rétt til að leggja á uppsafnað gjald vegna reglubrota, halda eftir greiðslum og/eða rifta Samningnum.

Kaflir 3

Stjórnunarskyldur vegna Gagnatilfella

Þér ber að gera American Express tafarlaust viðvart ef upp kemst um Gagnatilfelli og aldrei síðar en sjötíu og tveimur (72) klukkustundum eftir að upp kemst um það.

Til að gera American Express viðvart skaltu hafa samband við American Express Enterprise Incident Response Programme (EIRP) gjald-frjálst í síma 1.888.732.3750, eða í 1.602.537.3021, eða senda tölvupóst á EIRP@aexp.com. Þér ber að útnefna einstakling sem tengilið þinn vegna slíkra Gagnatilfella. Auk þess berð þú eftirfarandi skyldur:

- Þú verður að framkvæma vandlega rannsókn fyrir hvert Gagnatilfelli og láta American Express tafarlaust í té öll Kortanúmer sem stefnt var í hættu. American Express áskilur sér rétt til að gera eigin innri greiningu til að komast að því hvaða Kortanúmer voru hluti af Gagnatilvikinu.

Fyrir Gagnatilfelli sem varða færri en 10.000 einstök Kortanúmer þarf að veita American Express samantekt rannsóknar innan tíu (10) viðskiptadaga frá því henni er lokið.

- Samantektir rannsókna eiga að innihalda eftirfarandi upplýsingar: samantekt tilfellis, lýsingu á viðkomandi umhverfi, tímalínu atburða, lykildagsetningar, upplýsingar um áhrif afhjúpun gagna, afmörkunar- og úrbótaáðgerðir og staðfestingu að ekkert bendi til þess að frekari gögn American Express séu í hættu.

Fyrir Gagnatílfelli sem varða 10.000 eða fleiri einstök Kortanúmer þarft þú að ráða PCI PFI til að framkvæma þessa rannsókn innan fimm (5) daga eftir að Gagnatílfelli uppgötvast.

- Útvega þarf American Express óbreytta rannsóknarskýrslu innan tíu (10) viðskiptadaga frá því henni er lokið.
- Rannsóknarskýrslur skal fylla út með því að nota núverandi Sniðmát fyrir lokaskýrslur um gagnatílfelli sem PCI-aðili útvegar. Slík skýrsla verður að innihalda réttartæknilegar skoðanir, skýrslur um samræmisvottun og allar aðrar upplýsingar varðandi Gagnatílfellið. Auðkenndu ástæður Gagnatílfellisins, staðfestu hvort þú uppfylltir PCI DSS-staðalinn á tíma Gagnatílfellisins og sannreyndu getu þína til að koma í veg fyrir Gagnatílfelli í framtíðinni með því að (i) gera áætlun um úrbætur vegna allra tilfella þar sem misbrestur er á hlífingu við PCI DSS og (ii) taka þátt í áætlun American Express varðandi hlífingu (eins og lýst er að neðan). Samkvæmt beiðni American Express skalt þú útvega staðfestingu frá Viðurkenndum úttektaraðila (QSA) á því að bætt hafi verið úr öllum misbresti á hlífingu.

Óháð undanfarandi málsgreinum þessa [Kafli 3. „Stjórnunarskyldur vegna Gagnatílfella“](#):

- American Express getur, að eigin geðþóttu, krafist þess að þú ráðir PFI-rannsóknaraðila til þess að framkvæma rannsókn á Gagnatílfellum sem fela í sér færri en 10.000 einstök Kortanúmer eða þar sem mörg tilfelli hafa átt sér stað innan 12 mánaða tímabils. Allar slíkar rannsóknir verða að vera í samræmi við kröfur sem fram koma í þessum [Kafli 3. „Stjórnunarskyldur vegna Gagnatílfella“](#) og ljúka verður þeim innan þess tímaramma sem American Express segir fyrir um.
- American Express getur, að eigin geðþóttu, ráðið PFI-rannsóknaraðila sérstaklega til þess að framkvæma rannsókn á Gagnatílfellum og kann að skuldfæra kostnað slíkrar rannsóknar á þig.

Þér ber að meta Gagnatílfellið samkvæmt gildandi lögum um tilkynningar á gagnarofi á heimsvísu og, þar sem nauðsynlegt er talið, tilkynna viðeigandi eftirlitsaðilum og Korthöfum sem verða fyrir áhrifum í samræmi við slík lög um gagnarof. Ef þú hefur komist að þeirri niðurstöðu að Þjónustuveitandi þinn eða annar aðili sé ábyrgur fyrir því að tilkynna Gagnatílfellið, skalt þú kunngerá slíkum Þjónustuveitanda eða aðila um skyldu sína til að meta tilkynningarskyldu sína samkvæmt gildandi lögum um tilkynningar um gagnarof. Þú samþykkir að fá skriflegt samþykki frá American Express áður en þú vísar til eða nafngreinir American Express í hvers kyns samskiptum við Korthafa um Gagnatílfellið. Þú samþykkir að vinna með American Express að því að veita upplýsingar og ráða bót á öllum vandamálum sem koma upp í tengslum við Gagnatílfellið, þ.m.t. að veita (og afla allra nauðsynlegra undanþága til að geta veitt) American Express allar viðeigandi upplýsingar til að hægt sé að ganga úr skugga um að þú getir komið í veg fyrir Gagnatílfelli í framtíðinni, með þeim hætti sem samrýmist Samningnum.

Hvað sem líður gagnstæðum trúnaðarskyldum í Samningnum er American Express heimilt að veita upplýsingar um öll Gagnatílfelli til American Express-korthafa, Útgefenda, annarra þátttakenda í samstæðu American Express, og til almennings eins og skylt er samkvæmt Gildandi lögum, dómsúrskurði eða samkvæmt fyrirsmælum þar til bærra stjórnvalda eða á öðrum grundvelli til að draga úr hættu á svikum eða öðru tjóni eða með öðrum hætti að því marki sem við á til að unnt sé að starfrækja American Express netið.

Hvað skal gera ef Gagnatilvik kemur upp?

Fylgdu þessum skrefum ef Gagnatilvik greinist í fyrirtækinu þínu.

**Skref 1:**

Fylltu út [Frumtilkynningu um tilvik vegna gagna Söluaðila](#) og sendu hana með tölvupósti til EIRP@aexp.com innan 72 klukkustunda frá því að Gagnatilvikið greinist.

**Skref 2:**

Gerðu rannsókn – þú gætir þurft að ráða Rannsakanda [greiðslukortageirans \(PCI\)](#).

**Skref 3:**

Láttu okkur sem fyrst í té öll American Express® kortanúmer sem eru í hættu.

**Skref 4:**

Við hjálpum þér að leysa úr öllum vandamálum vegna Gagnatilviksins.

Skoðaðu [Kafli 3, „Stjórnunarskyldur vegna Gagnatilfella“](#) til að fá frekari upplýsingar um skyldur við meðferð Gagnatilvika.

Einhverjar spurningar?

Bandaríkin: (888) 732-3750 (gjaldfrjálst númer)

Önnur lönd: +1 (602) 537-3021

EIRP@aexp.com

Kafli 4**Skaðabótaskyldur vegna Gagnatilfella**

Skaðabótaskyldur þínar gagnvart American Express samkvæmt Samningnum um Gagnatilfelli skulu ákvarðaðar án þess að American Express afsali sér öðrum réttindum eða úrræðum samkvæmt þessum [Kafli 4, „Skaðabótaskyldur vegna Gagnatilfella“](#). Auk skaðabótaskyldna þinna (ef einhverjar eru) gætir þú þurft að greiða gjald vegna reglubrota vegna Gagnatilfella eins og lýst er neðar í þessum [Kafli 4, „Skaðabótaskyldur vegna Gagnatilfella“](#).

Þú þarft að greiða American Express bætur að upphæð 5\$ fyrir hvert reikningsnúmer, fyrir Gagnatilfelli sem ná til:

- 10.000 eða fleiri American Express-kortanúmera með öðru af eftirfarandi:
 - Viðkvæmum auðkenningargögnum eða
 - Gildistíma

Hins vegar mun American Express ekki leitast til þess að fá bætur frá þér fyrir Gagnatilvik sem ná til:

- færri en 10.000 American Express-kortanúmera eða
- fleiri en 10.000 American Express-kortanúmera ef eftirfarandi skilyrði eru uppfyllt:
 - þú hefur tilkynnt American Express um Gagnatilvikið í samræmi við [Kafli 3, „Stjórnunarskyldur vegna Gagnatilfella“](#),
 - þú uppfylltir kröfur PCI DSS-staðalsins á tíma Gagnatilviksins (samkvæmt niðurstöðu PFI-rannsóknaraðila á Gagnatilvikinu) og
 - Gagnatilvikið var ekki komið til vegna ólögsmæts athæfis þíns eða Tilgreindra aðila þinna.

Óháð undanfarandi efnisgreinum þessa [Kafli 4, „Skaðabótaskyldur vegna Gagnatilfella“](#), skalt þú greiða American Express gjald vegna reglubrots hvers konar Gagnatilviks, óháð fjölda American Express-kortanúmera, sem er að hámarki 100.000\$ fyrir hvert Gagnatilvik (samkvæmt ákvörðun American Express, að eigin geðþótta)

ef misbrestur verður á því að þú uppfyllir skyldur þínar samkvæmt [Kafli 3. „Stjórnunarskyldur vegna Gagnatílfella“](#). Til að forðast misskilning skal heildarupphæð gjalds vegna reglubrots staks Gagnatílvíks ekki vera hærri en 100.000\$.

American Express mun undanskilja í útreikningum sínum öll Reikningsnúmer American Express-korta sem voru hluti af fyrri bótakröfu vegna Gagnatílvíks innan tólf (12) mánaða fyrir Tilkynningardag. Allir útreikningar gerðir af American Express samkvæmt þessari aðferðafræði eru endanlegir.

American Express kann að rukka þig um heildarupphæð skaðabótaskyldna þinna vegna Gagnatílvíka eða draga upphæðina frá greiðslum American Express til þín (eða skuldfæra bankareikning þinn) samkvæmt Samningnum.

Skaðabótaskylda þín vegna Gagnatílfella hér undir skal ekki teljast vera tilfallandi, óbein, byggð á getgátum, afleidd, sérstök, til refsingar eða öðrum til varnaðar samkvæmt Samningnum, svo framarlega sem slíkar skyldur fela ekki í sér skaðabætur í tengslum við eða sem eru í eðli sínu vegna hagnaðar- eða tekjutaps, taps á viðskiptavild eða taps á viðskiptatækifærum.

American Express getur að eigin geðþótta lækkað skaðabótaskyldu Söluaðila eingöngu vegna Gagnatílfella sem uppfylla öll eftirfarandi skilyrði:

- Viðeigandi tækni til Áhættuminnkunar var í notkun fyrir Gagnatílfellið og var í notkun allan tímann meðan á Gagnatílfellinu stóð,
- lokið hefur verið ítarlegri rannsókn í samræmi við PFI-verkefnið (nema annað hafi verið samþykkt skriflega),
- það hafi komið skýrt fram í rannsóknarskýrslunni að Áhættuminnkandi tækni var notuð til að vinna úr, geyma og/eða senda gögnin á tíma Gagnatílfellisins, og
- þú geymir ekki (og geymdir ekki allan þann tíma sem Gagnatílfellið varði) Viðkvæm auðkenningargögn eða neinir Korthafaupplýsingar sem ekki hafa verið gerðar ólesanlegar.

Þar sem möguleiki er á lækkun skaðabóta verður lækkunin á skaðabótaskyldu þinni (að undanskildum gjöldum sem greiða skal vegna reglubrota) ákveðin á eftirfarandi hátt:

Tafla A-5: Nauðsynleg skilyrði fyrir lækkun skaðabótaskyldu

Lækkun skaðabótaskyldu	Nauðsynleg skilyrði
Venjuleg lækkun: 50%	>75% af öllum Færslum lesnum með Búnaði fyrir örflögu ¹ EDA
	Áhættuminnkandi tækni í notkun á >75% af staðsetningum Söluaðila ²
Aukin lækkun: 75% til 100%	>75% af öllum Færslum lesnum með Búnaði fyrir örflögu ¹ OG önnur Áhættuminnkandi tækni í notkun á >75% af staðsetningum Söluaðila ²

¹ Eins og ákveðið er samkvæmt innri greiningu American Express

² Eins og ákveðið er samkvæmt PFI-rannsókn

- Aukin lækkun (75% til 100%) skal vera ákveðin á grundvelli lægra prósentuhlutfalls Færslna með Búnaði fyrir örflögu OG staðsetningum Söluaðila sem nota aðra Áhættuminnkandi tækni. Dæmin í [Töflu A-6 Aukin lækkun skaðabótaskyldu](#) sýna útreikning á lækkun skaðabóta.
- Til að vera hæf(ur) fyrir Áhættuminnkandi tækni þá verður þú að sýna fram á markvissa notkun tækninnar í samræmi við hönnun hennar og ætlaðan tilgang.
- Hlutfall staðsetninga sem nota Áhættuminnkandi tækni er ákveðið með PFI-rannsókn.
- Lækkun skaðabótaskyldu gildir ekki um nein gjöld vegna reglubrota sem koma til greiðslu í tengslum við Gagnatílfellið.

Tafla A-6: Aukin lækkun skaðabótaskyldu

Dæmi	Áhættuminnkandi tækni í notkun	Kemur til greina	Lækkun
1	80% af Færslum með Búnaði fyrir örflögur 0% staðsetninga nota aðra Áhættuminnkandi tækni	Nei	50%: Venjuleg lækkun (minna en 75% notkun Áhættuminnkandi tækni gerir þig ekki hæfa(n) fyrir Aukna lækkun) ¹
2	80% af Færslum með Búnaði fyrir örflögur 77% staðsetninga nota aðra Áhættuminnkandi tækni	Já	77%: Aukin lækkun (byggð á 77% notkun Áhættuminnkandi tækni)
3	93% af Færslum með Búnaði fyrir örflögur 100% staðsetninga nota aðra Áhættuminnkandi tækni	Já	93%: Aukin lækkun (byggð á 93% af Færslum með Búnaði fyrir örflögur)
4	40% af Færslum með Búnaði fyrir örflögur 90% staðsetninga nota aðra Áhættuminnkandi tækni	Nei	50%: Venjuleg lækkun (minna en 75% af Færslum með Búnaði fyrir örflögur gerir þig ekki hæfa(n) fyrir Aukna lækkun)

¹ Gagnatílfelli með 10.000 reikningum American Express-korta, upp á 5\$ fyrir hvert reikningsnúmer (10.000 x 5\$ = 50.000\$) gæti komið til greina fyrir lækkun upp á 50% og lækkað þannig skaðabótaskylduna úr 50.000\$ í 25.000\$, að undanskildum öllum gjöldum vegna reglubrota.

Kafli 5

Áætlun um miðaða greiningu (TAP)

Stuldur á Korthafaupplýsingum getur verið vegna skorts á gagnaöryggi í Gagnaumhverfi korthafa (CDE).

Dæmi um stuld á Korthafaupplýsingum má nefna:

- **Sameiginlegir sölustaðir (CPP):** Korthafar American Express tilkynna um sviksamlegar Færslur á Kortareikningum þeirra og í ljós kemur að þær eiga uppruna sinn við innkaup í Fyrirtækinu þínu.
- **Korthafaupplýsingar fundust:** Korta- og Korthafaupplýsingar American Express fundust á veraldarefnum og tengjast Viðskiptum við Fyrirtæki þín.
- **Grunur um spilliforrit:** American Express grunar að þú notir hugbúnað sem er sýktur eða berskjaldaður gagnvart spilliforritum.

TAP er hannað til að koma auga á mögulegan gagnastuld Korthafaupplýsinga.

Þér ber að sjá til þess að þú og Tilgreindir aðilar þínir fari að eftirfarandi kröfum þegar tilkynning berst frá American Express um mögulegan stuld á Korthafaupplýsingum.

- Þú verður að leita að öryggisbresti í CDE og lagfæra tafarlaust.
 - Þú verður að sjá til þess að utanaðkomandi söluaðili/ar framkvæmi ítarlega skoðun á CDE ef það hefur verið útvistað.
- Þú verður að senda okkur samantekt á öllum aðgerðum, sem gripið hefur verið til eða grípa á til, út frá skoðuninni, matinu og/eða úrbótum þegar tilkynning um slíkt berst frá American Express.
- Þú verður að senda okkur uppfærð gögn um PCI DSS-staðfestingu í samræmi við [Kafli 2. „PCI DSS-samræmisáætlun \(mikilvæg reglubundin staðfesting á kerfum þínum\)“](#).
- Þú þarft, eftir því sem við á, að kalla til hæfan PCI PFI til að kanna CDE ef þú eða Tilgreindur aðili þinn:
 - Getur ekki leyst úr stuldi Korthafaupplýsinga innan eðlilegs tíma, að ákvörðun American Express, eða

- Staðfest að Gagnatilvik hafi átt sér stað og farið að kröfum í [Kafli 3. „Stjórnunarskyldur vegna Gagnatílfella“](#).

Tafla A-7: Gjald vegna reglubrota vegna TAP

Lýsing	Söluaðili á 1. stigi eða Þjónustu-veitandi á 1. stigi	Söluaðili á 2. stigi eða Þjónustu-veitandi á 2. stigi	Söluaðili á 3. stigi eða 4. stigi
Gjald fyrir reglubrot hugsanlega lagt á ef ekki er staðið við skuldbindingar í tengslum við TAP fyrir fyrsta skiladag.	25.000\$ Bandaríkjadalir	5.000\$ Bandaríkjadalir	1.000\$ Bandaríkjadalir
Gjald fyrir reglubrot hugsanlega lagt á ef ekki er staðið við skuldbindingar í tengslum við TAP fyrir annan skiladag.	35.000\$ Bandaríkjadalir	10.000\$ Bandaríkjadalir	2.500\$ Bandaríkjadalir
Gjald fyrir reglubrot hugsanlega lagt á ef ekki er staðið við skuldbindingar í tengslum við TAP fyrir þriðja skiladag. ATHUGIÐ: <i>Leggja má á Gjaldið fyrir reglubrot mánaðarlega þangað til staðið er við skuldbindingar eða leyst hefur verið úr TAP.</i>	45.000\$ Bandaríkjadalir	15.000\$ Bandaríkjadalir	5.000\$ Bandaríkjadalir

Ef ekki er staðið við skuldbindingar vegna TAP hefur American Express rétt til að leggja á uppsafnað gjald vegna reglubrota, halda eftir greiðslum og/eða rifta Samningnum.

Kafli 6

Þagnarskylda

American Express mun gera eðlilegar ráðstafanir til að gæta (og sjá til þess að umboðsmenn og undirverktakar sínir, þ.m.t. Gáttaveitan, gæti) trúnaðar um skýrslur þínar um samræmisvottun, þ.m.t. Staðfestingargögnin, og mun ekki birta staðfestingargögnin neinum þriðja aðila (öðrum en Hlutdeildarfélagum, umboðsmönnum, forsvarsmönnum, Þjónustuveitendum og undirverktökum American Express) í þrjú ár frá móttöku, með þeim fyrirvara að trúnaðarskyldan gildir ekki um Staðfestingargögn sem:

- a. American Express hafði vitneskju um áður en þau bárust;
- b. eru eða verða birt almenningi án nokkurs brots á þessari málsgrein af hálfu American Express;
- c. berast American Express frá þriðja aðila með lögleiðum leiðum án trúnaðarskyldu;
- d. útbúin eru af American Express; eða
- e. er skylt að birta samkvæmt úrskurði dómstóls, umsýsluskrifstofu eða stjórnvalds eða samkvæmt lögum, reglu, reglugerð eða stefnu, beiðni um upplýsingagjöf, kvaðningu eða öðru lagaferli eða með formlegri eða óformlegri fyrirspurn eða rannsókn stjórnvalds eða yfirvalds (þar með talið eftirlitsyfirvalds, rannsakanda, skoðanda eða löggæslufirvalda).

Kafli 7

Fyrirvari

AMERICAN EXPRESS HAFNAR ALLRI ÁBYRGÐ OG BÓTASKYLDU Í TENGLUM VIÐ ÞESSAR GAGNAÖRYGGISREGLUR, PCI DSS-STAÐALINN, EMV-FORSKRIFTINA OG SKIPUN OG FRAMMISTÖÐU VIÐURKENNDRA ÚTTEKTARAÐILA, VIÐURKENNDRA SKÖNNUNARAÐILA EÐA PFI-RANNSÓKNARAÐILA (EÐA EINHVERS ÞEIRRA), HVORT SEM ER BEINNI, AFLEIDDRI, LÖGBOÐINNI EÐA ANNARRI, Þ.M.T. ALLRI ÁBYRGÐ Á SÖLUHÆFI EÐA HÆFI FYRIR ÁKVEÐINN TILGANG. KORTHAFAR AMERICAN EXPRESS ERU EKKI ÞRÍÐJU AÐILAR SEM NJÓTA RÉTTINDA SAMKVÆMT ÞESSUM REGLUM.

Kafli 8

Orðalisti

Eftirfarandi skilgreiningar gilda um þessar *Reglur um gagnaöryggi*:

1. stigs Söluaðili er Söluaðili með 2,5 milljónir American Express-kortafærslna eða meira á ári eða hver sá Þjónustuveitandi sem American Express telur vera 1. stigs.

2. stigs Söluaðili er Söluaðili með 50.000 til færri en 2,5 milljónir American Express-kortafærslur á ári.

3. stigs Söluaðili er Söluaðili með 10.000 til færri en 50.000 American Express-kortafærslur á ári.

4. stigs Söluaðili er Söluaðili með færri en 10.000 American Express-kortafærslur á ári.

1. stigs Þjónustuveitandi er Þjónustuveitandi sem vinnur úr 2,5 milljónum eða fleiri American Express-kortafærslum á ári eða hver sá Þjónustuveitandi sem American Express telur vera 1. stigs.

2. stigs Þjónustuveitandi er Þjónustuveitandi sem er með færri en 2,5 milljónir American Express-kortafærslur á ári eða hver sá Þjónustuveitandi sem American Express telur ekki vera 1. stigs.

Áhættuminnkandi tækni eru tæknilausnir sem auka öryggi American Express-korthafaupplýsinga og Viðkvæmra auðkenningargagna samkvæmt ákvörðun American Express. Til að vera hæf(ur) fyrir Áhættuminnkandi tækni þá verður þú að sýna fram á markvissa notkun tækninnar í samræmi við hönnun hennar og ætlaðan tilgang. Dæmi um slíkt eru, en takmarkast ekki við: EMV, Dulkóðun frá punkti til punkts og merkning.

American Express-kort, eða **Kort**, merkir sérhvert kort, reikningsaðgangstæki, greiðslutæki eða þjónustu sem ber nafn, kennimerki, vörumerki, þjónustumerki eða viðskiptaheiti American Express eða aðra réttindavarða hönnun eða tilgreiningu og sem er gefið út af útgefanda eða kortareikningsnúmeri.

Áætlun um aukna öryggistækni (STEP) er áætlun American Express sem hvetur Söluaðila til að taka í notkun tækni sem eykur gagnaöryggi.

Áætlun um miðaða greiningu er áætlun sem býður upp á skjóta greiningu mögulegs stulds á Korthafaupplýsingum í Gagnaumhverfi korthafa (CDE). Sjá [Kafli 5. „Áætlun um miðaða greiningu \(TAP\)“](#).

Áætlunin þýðir American Express PCI-samræmisáætlun.

BIP-færslur (Buyer Initiated Payments) er stafræn greiðslulausn sem gerir kaupendum kleift að skipuleggja greiðslur til söluaðila á fljótan og skilvirkan hátt (tengt við fyrirtækjakort).

Búnaður fyrir örflögur er posi sem er með gilda og nýjustu útgáfu af EMVCo-auðkenningar/-vottun (www.emvco.com) og sem getur unnið úr Flögukortafærslum sem uppfylla AEIPS.

Dulkóðunarlykill („American Express dulkóðunarlykill“) er hver sá lykill sem notaður er við úrvinnslu, framleiðslu, hleðslu og/eða vörn reikningsgagna. Slíkir lykilar eru meðal annars, en ekki einvörðungu:

- Lykladulkóðunarlyklar: Svæðisaðallyklar (ZMK) og Svæðispinnlyklar (ZPK)
- Aðallyklar sem eru notaðir í öruggum dulkóðunartækjum: Staðbundnir aðallyklar (LMK)
- Kortaöryggiskóðalyklar (CSCK)
- PIN-lyklar: Grunnafleiðslulyklar (BDK), PIN-dulkóðunarlyklar (PEK) og ZPK-lyklar

Dulkóðun frá punkti til punkts (P2PE) er lausn sem verndar gögn reiknings með dulkóðun frá þeim punkti sem söluaðili samþykkir greiðslukortið og til hins örugga punkts afkóðunar.

EMV forskrift er forskriftin sem er gefin út af EMVCo, LLC, og er fánleg á www.emvco.com.

EMV færsla er Færsla með innbyggðu flögukorti (stundum kallað „IC-kort“, „flögukort“, „snjallkort“, „EMV-kort“, eða „ICC“) sem fer fram á posa sem getur tekið á móti IC-korti og er með gilda EMV-gerðarviðurkenningu. EMV-gerðarviðurkenning fæst á www.emvco.com.

Endurgreiðsla er upphæð Færslu sem er endurgreidd Korthafa fyrir kaup eða greiðslur með Korti.

Endurgreiðsluskrá er skrá yfir Endurgreiðslur sem eru í samræmi við kröfur okkar.

Flaga er innbyggð örflaga sem er felld inn í Kort og sem inniheldur upplýsingar um Korthafa og reikning.

Flögukort er Kort sem er með Flögu og kann að þurfa PIN-númer til að sannreyna auðkenni Korthafans eða reikningsupplýsingar sem finnast á Flögunni, eða bæði (stundum kallað „snjallkort“, „EMV-kort“ eða „ICC“ eða „innbyggt flögukort“ í gögnum okkar.)

Færsla er Gjaldfærsla, Endurgreiðsla, Fyrirframgreiðsla í reiðufé (eða annar aðgangur að reiðufé), eða hraðbankafærsla með Korti.

Færsluhirðir merkir þjónustuveitandi fyrir Söluaðila sem annast heimildaveitingu og vinnslu á sendingum til netkerfis American Express.

Færslugögn eru allar upplýsingar sem krafist er af American Express til að sýna fram á eina eða fleiri Viðskiptafærslu, þar á meðal upplýsingar sem aflað er á sölustað, upplýsingar sem aflað er eða myndast við Heimildaveitingu og Vinnslu eða Bakfærslu.

Gagnatilvik er tilvik sem felur í sér að dulkóðunarlyklum American Express er stolið, eða grun um stuld á þeim, eða a.m.k. eitt reikningsnúmer American Express-korts sem eftirfarandi á við um:

- óleyfilegur aðgangur eða notkun á Dulkóðunarlyklum, Korthafaupplýsingum eða Viðkvæmum auðkenningargögnum (eða samsetningu þessa) sem geymd eru, unnið er úr eða send eru með búnaði þínum, kerfum og/eða netkerfum þínum (eða hlutum þeirra) eða notkun þeirra sem þú fyrirskipar; veitir eða gerir aðgengilega;
- notkun slíkra Dulkóðunarlykla, Korthafaupplýsinga eða Viðkvæmra auðkenningargagna (eða samsetningar þeirra) að öðru leyti en í samræmi við Samninginn; og/eða
- grunur um eða staðfesting á því að efni, skrár eða upplýsingar sem geyma slíka Dulkóðunarlykla, Korthafaupplýsingar eða Viðkvæm auðkenningargögn (eða samsetningu þeirra) hafi tapast, verið stolið eða misnotuð á einhvern hátt.

Gagnaöryggisstaðall greiðslukortafyrirtækja (PCI DSS) þýðir Gagnaöryggisstaðall greiðslukortafyrirtækja en hann má finna á www.pcisecuritystandards.org.

Gagnaumhverfi korthafa (CDE) á við um fólk, ferli og tækni sem geymir, vinnur úr eða sendir korthafaupplýsingar eða viðkæm sannvottunargögn.

Gátt merkir skýrslukerfið sem stjórnandi American Express PCI-áætlunar hefur valið af American Express. Söluaðilar og þjónustuveitendur þurfa að nota Gáttina til að leggja fram PCI Staðfestingargögn til American Express.

Gjaldfærsla er greiðsla eða kaup framkvæmd með Korti.

Greiðsluumsókn hefur þá merkingu sem fram kemur í Orðalista fyrir Öryggisstaðal Hugbúnaðar og Öryggisstaðal fyrir Endingarskeið Hugbúnaðar, sem sjá má á www.pcisecuritystandards.org.

Kortanúmer þýðir einkvæmt auðkennisnúmer sem útgefandinn gefur Kortinu þegar það er gefið út.

Kortanúmer í hættu er American Express-kortareikningsnúmer sem tengist Gagnatilfelli.

Kortaútgefandi þýðir Aðili (þar á meðal American Express og Hlutdeildarfélag þess) með leyfi frá American Express eða hlutdeildarfélagi American Express til að gefa út Kort og taka þátt í kortaútgáfuviðskiptum.

Korthafaupplýsingar eru upplýsingar um Korthafa American Express og Kortafærslur þeirra, þar á meðal nöfn, heimilisföng, reikningsnúmer korta og CID-kortanúmer.

Korthafaupplýsingar eru að lágmarki allt Reikningsnúmerið (PAN) eitt og sér eða allt PAN-númerið ásamt einhverju af eftirfarandi: nafni korthafa, gildistíma, og/eða þjónustukóða. Sjá Viðkvæm auðkenningargögn fyrir viðbótargagnaþætti sem gætu verið sendir eða unnir (en ekki geymdir) sem hluti af greiðslufærslu.

Korthafi er einstaklingur eða aðili (i) sem hefur gert samning um að stofna til Kortareiknings hjá útgefanda eða (ii) hvers nafn kemur fram á Kortinu.

Korthafi er viðskiptavinur sem greiðslukort er gefið út til eða hver sá einstaklingur sem hefur heimild til að nota greiðslukortið.

Kröfur Öryggisstaðlaraðs greiðslukortafyrirtækja (PCI SSC) eru staðlar og kröfur um öryggi og vernd greiðslukortaupplýsinga, þ.m.t. PCI DSS og PA DSS sem finna má á www.pcisecuritystandards.org.

Kvittun er skrá sem unnt er að endurskapa (bæði á pappír og rafrænt) yfir Gjaldfærslu sem er í samræmi við kröfur okkar og inniheldur Kortanúmer, Viðskiptadagsetningu, upphæð, Samþykki, undirskrift Korthafa (ef við á) og aðrar upplýsingar.

Merking þýðir dulkóðunartáknið sem kemur í stað PAN, byggt á tiltekinni vísitölu fyrir ófyrirsjáanlegt gildi.

Neytandi er skilgreindur sem korthafi sem kaupir vörur, þjónustu eða hvort tveggja.

PCI DSS er Gagnaöryggisstaðall greiðslukortafyrirtækja sem nálgast má á www.pcisecuritystandards.org.

PCI-rannsóknaraðili (PFI) er aðili sem hefur fengið samþykki Öryggisstaðlaraðs greiðslukortafyrirtækja, LLC, til að framkvæma rannsóknir á broti eða stuldi á Greiðslukortaupplýsingum.

PCI-vottað merkir að PIN-innsláttartæki eða Greiðsluforrit (eða hvort tveggja) koma fram, er þau voru tekin í notkun, á listanum yfir vottuð fyrirtæki og veitendur sem PCI-öryggisstaðlaraðið, LLC, heldur úti og finna má á www.pcisecuritystandards.org.

PCI PIN-öryggiskröfur eru PIN-öryggiskröfur greiðslukortafyrirtækja sem sjá má á www.pcisecuritystandards.org.

PIN-innsláttartæki hefur þá merkingu sem fram kemur í Orðalista fyrir öryggiskröfur greiðslukortafyrirtækja vegna PIN-viðskiptafærslu (PIN Transaction Security - PTS) og samskiptatækja (Point of Interaction - POI), sem sjá má á www.pcisecuritystandards.org.

Posakerfi (POS) er kerfi eða búnaður sem vinnur úr upplýsingum, þ.m.t. kortalesari, tölva, rafrænn afgreiðslukassi, snertifrjáls lesari eða greiðsluvél eða -ferli sem Söluaðili notar til að fá heimild eða til að safna Færslugögnum, eða hvort tveggja.

Reikningsgögn samanstanda af Korthafaupplýsingum og/eða Viðkvæmum auðkenningargögnum. Sjá Korthafaupplýsingar og Viðkvæm auðkenningargögn.

Reikningsnúmer (PAN) hefur þá merkingu sem því er gefin í þágildandi Orðalista yfir skilmála fyrir PCI DSS.

Samningur þýðir almenn ákvæði, Reglur fyrir Söluaðila og allar meðfylgjandi áætlanir og sönnunargögn í heild (stundum vísað til sem Samningurinn um kortasamþykki í efni okkar).

Sérleyfisgjafi þýðir fyrirtæki i einkaeigu, sem starfrækt er að utanaðkomandi aðila (þar á meðal Sérleyfisgjafi, leyfishafi eða deild) annað en Hlutdeildarfyrirtæki, með leyfi frá Sérleyfisgjafa um að starfrækja sérleyfisfyrirtækið og sem gert hefur skriflegan samning við Sérleyfisgjafann. Sérleyfishafinn skuldbindur sig til að koma fyrir sérstöku auðkenni á áberandi stað með Vörumerkjum Sérleyfisgjafans eða koma fram fyrir almenning sem aðili í fyrirtækjasamstæðu Sérleyfisgjafans.

Sérleyfisveitandi er rekstraraðili fyrirtækis sem veitir einstaklingum eða Fyrirtækjum (Sérleyfishöfum) leyfi til að dreifa vörum og/eða þjónustu eða stunda rekstur undir Merkjum rekstraraðilans, og sem veitir Sérleyfishöfum aðstoð við rekstur fyrirtækja þeirra eða hefur áhrif á aðferðir Sérleyfishafans við reksturinn, og krefur Sérleyfishafann um greiðslu gjalds.

Sjálfsmatsspurningalisti (SAQ) er aðferð til sjálfsmats, útbúin af Öryggisstaðlaraði greiðslukortafyrirtækja, LLC, með það að markmiði að meta og votta hlífingu við PCI DSS.

Sniðmát fyrir Lokaskýrslu merkir sniðmátið sem er fánlegt frá PCI-öryggisstaðlaraði, sem er fánlegt á www.pcisecuritystandards.org.

Staðfestingargögn merkir AOC-eyðublað sem er útbúið í tengslum við Árlegt öryggismat á vettvangi eða SAQ, AOSC-skýrslan og samantektir á niðurstöðum Ársfjórðungslegrar netkerfisskönnunar eða Árleg staðfesting áætlunar um aukna tækni.

Staðfesting um Samræmisvottun (AOC) er yfirlýsing um stöðu hlífingar við PCI DSS-staðalinn á eyðublaði sem gefið er út af Öryggisstaðlaraði greiðslukortafyrirtækja, LLC.

Stig Söluaðila merkir þá tilnefningu sem við úthlutum Söluaðilum í tengslum við PCI DSS staðfestinguna, eins og lýst er í [Kafli 2. „PCI DSS-samræmisáætlun \(mikilvæg reglubundin staðfesting á kerfum þínum\)“](#).

Söluaðili er Söluaðilinn og öll hlutdeildarfélög hans sem taka við American Express-kortum samkvæmt Samningi við American Express eða hlutdeildarfélög þess.

Tilgreindir aðilar eru einhverjir eða allir starfsmenn þínir, umboðsmenn, fulltrúar, undirverktakar, Færsluhirðar, Þjónustuveitendur, veitendur Posabúnaðar (POS) eða kerfa eða lausna við framkvæmd greiðslna, aðilar sem tengjast American Express-Söluaðilareikningi þínum og hverskyns aðrir aðilar sem þú gætir veitt aðgang að Korthafaupplýsingum eða Viðkvæmum auðkenningagögnum (eða bæði) í samræmi við Samninginn.

Tilkynningardagur er sá dagur sem American Express veitir útgáfuaðilum lokatilkynningu um Gagnatilfelli. Slík dagsetning er háð því hvenær American Express móttækur lokaskýrsluna um gagnatilfellið eða innri greininguna og er ákveðin af American Express að eigin geðþóttu.

Tími sem gagnatilfelli varir er tímabil stuldar (eða álíka ákveðið tímabil) sem fram kemur í lokaskýrslunni um gagnatilfelli (t.d. PCI skýrslu), eða ef óþekkt, allt að 365 dögum fyrir síðustu Dagsetningu tilkynningar af Kortanúmeri í hættu í tengslum við stuld á Upplýsingum sem okkur hefur verið tilkynnt.

Viðkvæm auðkenningargögn eru öryggistengdar upplýsingar sem notaðar eru til að auðkenna korthafa og/eða heimila greiðslukortafærslur. Þessar upplýsingar innihalda, en takmarkast ekki við, sannprófunarkóða korta, öll rekjanleg gögn (frá segulrönd eða samsvarandi á örflögu), PIN-númer og PIN-blokkir.

Viðurkennd dulkóðunarlausn frá punkti til punkts (P2PE), á lista PCI SSC yfir staðfestar lausnir eða er staðfest af PCI SSC-viðurkenndu P2PE-úttektarfyrtækki.

Viðurkenndur skönnunaraðili (ASV) er Aðili sem hefur verið viðurkenndur af Öryggisstaðlaraði greiðslukortafyrirtækja, LLC til að staðfesta fylgni við ákveðnar PCI DSS-kröfur með því að framkvæma skönnun fyrir veikleikum í netumhverfum.

Viðurkenndur úttektaraðili (QSA) er aðili sem hefur verið viðurkenndur af Öryggisstaðlaraði greiðslukortafyrirtækja, LLC til að staðfesta hlítinu við PCI DSS-staðalinn.

Vottun á skönnunarhlítinu (AOSC) er yfirlýsing um stöðu hlítinu þinnar við PCI DSS-staðalinn, byggt á netkerfisskönnun, á eyðublaði sem gefið er út af Öryggisstaðlaraði greiðslukortafyrirtækja, LLC.

Þjónustuveitendur eru samþykktir færsluhirðar, utanaðkomandi færsluhirðar, gáttarveitendur og aðrir sem veita Söluaðilum posabúnað, hugbúnað eða kerfi eða aðrar greiðsluvinnslulausnir eða þjónustu.

Kafli 9

Gagnleg vefsvæði

Gagnaöryggi American Express: www.americanexpress.com/datasecurity

Öryggisstaðlaraði greiðslukortafyrirtækja, LLC: www.pcisecuritystandards.org

EMVCo: www.emvco.com