AMERICAN EXPRESS

Reglur um gagnaöryggi (DSOP)

Breytingartákn

Mikilvægar uppfærslur eru taldar upp í Samantektartöflunni yfir breytingar en þær eru einnig sýndar í *DSOP* með breytingartákni. Breytingartákn við hliðina á kaflaheiti eða undirkaflaheiti sýnir að texti í kaflanum eða undirkaflanum hefur verið endurskoðaður, bætt hefur verið við hann eða texta eytt úr honum. Breytingar á *DSOP* eru sýndar með breytingartákni eins og sýnt er hér.

Samantektartafla yfir breytingar

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

Kafli/undirkafli	Lýsing á breytingu
Kafli 1, „Áætlun um miðaða greiningu (TAP)“	• Heiti á kafla 1 breytt úr „Stuldur á Korthafaupplýsingum“ í „Áætlun um miðaða greiningu (TAP)“. • Skýrara orðalag.
Orðalisti	• Uppfært orðalag vegna gagnatilfella. • Skilgreiningum bætt við fyrir Gagnaumhverfi korthafa og Áætlun um miðaða greiningu.

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, 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.

Kafli 1 Áætlun um miðaða greiningu (TAP)

Stuldur á Korthafaupplýsingum getur verið vegna skorti 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 5, „Mikilvæg reglubundin staðfesting á kerfum þínum“.
- Þú þarft, eftir því sem við á, að kalla til hæfan PCI rannsóknaraðila (PFI) til að kanna Gagnaumhverfi korthafa ef þú eða Tilgreindur aðili þinn:
  - Getur ekki leyst úr Stuldi korthafaupplýsinga innan eðlilegs tíma, að ákvörðun American Express, eða
  - Staðfesta að Gagnatilvik hafi átt sér stað og farið að kröfum í Kafli 3, „Stjórnunarskyldur vegna gagnatilfella“.

Gjald vegna reglubrota vegna TAP

Lýsing	Söluaðili á 1. stigi eða Þjónustuveitandi á 1. stigi	Söluaðili á 2. stigi eða Þjónustuveitandi á 2. stigi	Söluaðili á 3. eða 4. stigi
Gjald fyrir reglubrot lagt á ef ekki er staðið við skuldbindingar í tengslum við TAP innan 45 daga frá tilkynningardagsetningu.	25.000$ Bandaríkjadalir	5.000$ Bandaríkjadalir	1.000$ Bandaríkjadalir
Gjald fyrir reglubrot lagt á ef ekki er staðið við skuldbindingar í tengslum við TAP innan 90 daga frá tilkynningardagsetningu.	35.000$ Bandaríkjadalir	10.000$ Bandaríkjadalir	2.500$ Bandaríkjadalir
Gjald fyrir reglubrot lagt á ef ekki er staðið við skuldbindingar í tengslum við TAP innan 120 daga frá tilkynningardagsetningu. **ATHUGIÐ:** *Leggja má á Gjaldið fyrir reglubrot mánaðarlega þangað til staðið er við skuldbindingar eða leyst hefur verið úr TAP.*	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 2 Staðlar sem gilda um Vernd dulkóðunarlykla, Korthafaupplýsinga og Viðkvæmra auðkenningargagna

Þér ber að gera eftirfarandi og sjá til þess að Tilgreindir aðilar þínir geri það líka:

- geyma Korthafaupplýsingar aðeins í því skyni að greiða fyrir viðskiptum 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 Korthafaupplýsinga eða Viðkvæmra auðkenningargagna eigi síðar en þann dag sem sú útgáfa viðkomandi kröfu tók gildi.
- nota, þegar PIN-innsláttartæki eða Greiðsluforrit (eða bæði) sem eru ný eða koma í stað annarra eru tekin í notkun, aðeins þau sem eru PCI-viðurkennd.

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 5, „Mikilvæg reglubundin staðfesting á kerfum þínum“).

Kafli 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*) í síma +1 (602) 537-3021 (+ er alþjóðlega forskeytið vegna beinna hringinga, alþjóðleg símagjöld gilda) eða í tölvupósti 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 réttartæknilega rannsókn fyrir hvert Gagnatilfelli.

- Fyrir Gagnatilfelli sem varða 10.000 eða fleiri einstök Kortanúmer þarft þú að ráða PCI-rannsóknaraðila (PFI) til að framkvæma þessa rannsókn innan fimm (5) daga eftir að Gagnatilfelli uppgötvast.
- Útvega þarf American Express óbreytta rannsóknarskýrslu innan tíu (10) daga frá því henni er lokið.
- Þér ber að láta American Express tafarlaust í té öll þau 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.

Fylla skal út réttartæknilegar rannsóknarskýrslur með því að nota núverandi Sniðmát fyrir lokaskýrslu um gagnatilfelli sem PCI-aðili útvegar. Slík skýrsla verður að innihalda réttartæknilegar skoðanir, skýrslur um hlítingu og allar aðrar upplýsingar varðandi Gagnatilfellið. Auðkenndu ástæður Gagnatilfellisins, staðfestu hvort þú uppfylltir PCI DSS-staðalinn á tíma Gagnatilfellisins og sannreyndu getu þína til að koma í veg fyrir Gagnatilfelli í framtíðinni með því að (i) gera áætlun um úrbætur vegna allra tilfella þar sem misbrestur er á hlítingu við PCI DSS og (ii) taka þátt í áætlun American Express varðandi hlítingu (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 hlítingu.

Óháð undanfarandi málsgreinum þessa Kafli 3, „Stjórnunarskyldur vegna gagnatilfella“:

- American Express getur, að eigin geðþótta, krafist þess að þú ráðir PFI-rannsóknaraðila til þess að framkvæma rannsókn á Gagnatilfellum sem fela í sér minna en 10.000 einstök kortanúmer. Allar slíkar rannsóknir verða að vera í samræmi við kröfur sem fram koma í þessum Kafli 3, „Stjórnunarskyldur vegna gagnatilfella“ og ljúka verður þeim innan þess tímaramma sem American Express segir fyrir um.
- American Express getur, að eigin geðþótta, ráðið PFI-rannsóknaraðila sérstaklega til þess að framkvæma rannsókn á Gagnatilfellum og kann að skuldfæra kostnað slíkrar rannsóknar á þig.

Þú samþykkir að vinna með American Express að því að ráða bót á öllum vandamálum sem koma upp í tengslum við Gagnatilfellið, þ.m.t. að ráðfæra þig við American Express varðandi samskipti þín við Korthafa sem hafa orðið fyrir áhrifum af Gagnatilfellinu og 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 Gagnatilfelli í framtíðinni, með þeim hætti sem samrýmist Samningnum.

Hvað sem líður gagnstæðum trúnaðarskyldum í Samningnum er American Express heimilt að veita upplýsingar um öll Gagnatilfelli til American Express-korthafa, Útgefenda, annarra þátttakenda í samstæðu American Express, og til almennings eins og skylt er samvkæmt Gildandi lögum, dómsúrskurði eða samkvæmt fyrirmælum 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.

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 gjöld vegna misbrests á hlítingu vegna Gagnatilviks eins og lýst neðar í þessum Kafli 4, „Skaðabótaskyldur vegna Gagnatilfella“.

Fyrir Gagnatilvik sem ná til:

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

  þarft þú að greiða American Express bætur að upphæð 5 USD fyrir hvert reikningsnúmer.

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 10.000 American Express-kortanúmera ef eftirfarandi skilyrði eru uppfyllt:
  - þú hefur tilkynnt American Express um Gagnatilvikið í samræmi við þennan Kafli 4, „Skaðabótaskyldur vegna Gagnatilfella“,

- þú uppfylltir kröfur PCI DSS-staðalsins á tíma Gagnatilviksins (samkvæmt niðurstöðu PFI-rannsóknaraðila á Gagnatilvikinu), og
- Gagnatilvikið var ekki komið til vegna ólögmæts athæfis þíns eða Tilgreindra aðila þinna.

Óháð undanfarandi efnisgreinum þessa Kafli 4, „Skaðabótaskyldur vegna Gagnatilfella", skalt þú greiða American Express gjald vegna misbrests á hlítingu vegna hvers konar Gagnatilviks, óháð fjölda American Express-kortanúmera, sem er að hámarki 100.000 USD 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 gagnatilfella". Til að forðast misskilning skal heildarupphæð gjalds vegna misbrests á hlítingu vegna staks Gagnatilviks ekki vera hærri en 100.000 USD.

American Express mun undanskilja í útreikningum sínum öll Reikningsnúmer American Express-korta sem voru hluti af fyrri bótakröfu vegna Gagnatilviks 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 Gagnatilvika eða draga upphæðina frá greiðslum American Express til þín (eða skuldfæra Bankareikning þinn) samkvæmt Samningnum.

Skaðabótaskylda þín vegna Gagnatilfella 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 Gagnatilfella sem uppfylla öll eftirfarandi skilyrði:

- Viðeigandi tækni til Áhættuminnkunar var í notkun fyrir Gagnatilfellið og var í notkun allan tímann meðan á Gagnatilfellinu 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 Gagnatilfellisins, og
- þú geymir ekki (og geymdir ekki allan þann tíma sem Gagnatilfellið varði) Viðkvæm auðkenningargögn eða neinar 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 misbrests hlítingu) ákveðin á eftirfarandi hátt:

Lækkun skaðabótaskyldu	Nauðsynleg skilyrði
Venjuleg lækkun: 50%	>75% af öllum Færslum lesnum með Búnaði fyrir örflögu[1] EÐA
	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 fyrir neðan útskýra 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. Til dæmis er það EKKI markviss notkun þessarar tækni að taka í notkun Búnað fyrir örflögur en nota síðan Segulrönd eða Skráningu með lyklaborði fyrir færslur korta sem eru með örflögu.
- Hlutfall staðsetninga sem nota Áhættuminnkandi tækni er ákveðið með PFI-rannsókn.

- Lækkun skaðabótaskyldu gildir ekki um nein gjöld vegna misbrests á hlítingu sem koma til greiðslu í tengslum við Gagnatilfellið.

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% notkun Búnaðar fyrir örflögur gerir þig ekki hæfa(n) fyrir Aukna lækkun)

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

Kafli 5 Mikilvæg reglubundin staðfesting á kerfum þínum

Þér ber að grípa til eftirfarandi aðgerða til að staðfesta, árlega og ársfjórðungslega 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 áætlun American Express varðandi hlítingu við þessar reglur.

Aðgerð 2: Hafðu skilning á Stigi þínu og Staðfestingarkröfum.

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

1. stigs söluaðilar, 2. stigs Söluaðilar og allir Þjónustuveitendur, eins og lýst er að neðan, verða að taka þátt í PCI-áætlun American Express varðandi hlítingu samkvæmt þessum reglum með því að gefa upp fullt nafn, netfang, símanúmer og póstfang einstaklings sem mun gegna starfi gagnaöryggistengiliðs. Þér ber að senda þessar upplýsingar til SecureTrust, deild innan Trustwave (https://portal.securetrust.com), þar sem áætluninni er stýrt fyrir hönd American Express, með einni af þeim leiðum sem lýst er í Aðgerð 4: „Staðfestingargögn send til American Express“ hér að neðan. Þér ber að tilkynna SecureTrust ef breytingar verða á þessum upplýsingum og veita nýjar upplýsingar ef þörf krefur. Veitir þú ekki slíkar tengiliðaupplýsingar hefur það ekki áhrif á rétt okkar til að meta gjöld fyrir ógildingu samkvæmt Tafla yfir ógildingargjöld.

American Express getur að eigin geðþótta tilnefnt að 3. stigs og 4. stigs Söluaðilar taki þátt í áætlun American Express um reglufylgni samkvæmt þessari stefnu með því að senda þeim skriflega tilkynningu. Söluaðilinn verður að skrá sig ekki síðar en 90 dögum eftir móttöku tilkynningarinnar.

Aðgerð 2: Hafðu skilning á stigi þínu og Staðfestingarkröfum

Hér eru fjögur stig til notkunar fyrir Söluaðila og tvö stig til notkunar fyrir Þjónustuveitendur sem byggjast á þínu magni af American Express-kortafærslum. Fyrir Söluaðila er þetta það magn sem sent er inn af fyrirtæki þeirra sem nær upp til hæsta stigs fyrir American Express reikning Söluaðila.* Þú munt falla undir eitt af Stigunum sem tilgreind eru í töflunum fyrir Söluaðila og Þjónustuveitendur að neðan. BIP-færslur (Buyer Initiated Payments) eru ekki innifaldar í magni American Express-kortafærslna til að ákvarða Stig söluaðila eða staðfestingarkröfur.

* Í tilfelli Sérleyfisveitenda þá innifelur þetta magnið frá fyrirtækjum Sérleyfishafa þeirra. Sérleyfisveitendur sem fyrirskipa Sérleyfishöfum sínum að nota ákveðið Posakerfi (POS) eða Þjónustuveitanda verða einnig að útvega staðfestingargögn fyrir viðkomandi Sérleyfishafa.

Kröfur til Söluaðila

Söluaðilar (ekki Þjónustuveitendur) skiptast í fjóra flokka hvað varðar stig þeirra og staðfestingarkröfur. Eftir að stig Söluaðila hefur verið ákvarðað á grundvelli upptalningarinnar hér að neðan má sjá hvaða kröfur eru gerðar varðandi staðfestingargögn í Söluaðilatöflunni.

- **1. stigs Söluaðili** – 2,5 milljón American Express-kortafærslur eða meira á ári, eða hver sá þjónustuveitandi sem American Express útnefnir sem 1. stigs.
- **2. stigs Söluaðili** – 50.000 til 2,5 milljón American Express-kortafærslur á ári.
- **3. stigs Söluaðili** – 10.000 til 50.000 American Express-kortafærslur á ári.
- **4. stigs Söluaðili** – minna en 10.000 American Express-kortafærslur á ári.

Söluaðilatafla

	Staðfestingargögn		
Stig Söluaðila/ Árlegar American Express-færslur	Matsskýrsla um hlítingu á vettvangi (ROQ)	Sjálfsmatsspurningarlisti (SAQ) OG ársfjórðungsleg netskönnun	STEP-vottun fyrir gjaldgenga Söluaðila
1. stig/ 2,5 milljónir eða fleiri	Skylda	Á ekki við	Valkvætt (kemur í stað ROC)
2. stig/ 50.000 til 2,5 milljónir	Valkvætt	SAQ er skylda (nema vettvangsmat sé sent inn); skönnun er skylda í tengslum við tilteknar gerðir SAQ	Valkvætt (kemur í stað SAQ og netkerfisskönnunar eða ROC)
3. stig/ 10.000 til 50.000	Valkvætt	SAQ er valkvætt (skylda ef American Express fer fram á það); skönnun er skylda í tengslum við tilteknar gerðir SAQ	Valkvætt (kemur í stað SAQ og netkerfisskönnunar eða ROC)
4. stig/ 10.000 eða færri	Valkvætt	SAQ er valkvætt (skylda ef American Express fer fram á það); skönnun er skylda í tengslum við tilteknar gerðir SAQ	Valkvætt (kemur í stað SAQ og netkerfisskönnunar eða ROC)

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

American Express áskilur sér rétt til að eftir þörfum sannreyna að PCI-staðfestingargögn sem veitt eru séu rétt og viðeigandi, þ.m.t. með því að ráða, á kostnað American Express, QSA eða PFI-rannsóknaraðila að okkar vali.

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:

- **EMV** – í Tæki sem tekur við flögum sem er með gilda og nýjustu útgáfu af EMVCo-auðkenningu/-vottun (www.emvco.com) og sem getur unnið úr Flögukortafærslum sem uppfylla AEIPS. (Bandarískir söluaðilar verða að styðja Snertilausar greiðslur)
- **Dulkóðun frá punkti til punkts (P2PE)** – send í örgjörva Söluaðila með PCI-SCC-viðurkenndu eða QSA-viðurkenndu Dulkóðunarkerfi frá punkti til punkts

Kröfur um PCI-staðfestingargögn eru minni fyrir Söluaðila sem eru gjaldgengir fyrir STEP, eins og nánar er lýst í Aðgerð 3: „Klárað Staðfestingargögnin sem þú þarft að senda American Express“ hér að neðan.

Kröfur til Þjónustuveitenda

Þjónustuveitendur (ekki Söluaðilar) skiptast í tvo flokka hvað varðar stig þeirra og staðfestingarkröfur. Eftir að stig Þjónustuveitanda hefur verið ákvarðað á grundvelli upptalningarinnar hér að neðan má sjá hvaða kröfur eru gerðar varðandi staðfestingargögn í Þjónustuveitendatöflunni.

1. stigs Þjónustuveitandi – Þjónustuveitandi sem vinnur úr yfir 2,5 milljónum American Express-kortafærslna á ári eða hver sá Þjónustuveitandi sem American Express telur vera 1. stigs.

2. stigs Þjónustuveitandi – Þjónustuveitandi sem vinnur úr færri en 2,5 milljónum American Express-kortafærslna á ári eða hver sá Þjónustuveitandi sem American Express telur ekki vera 1. stigs.

Þjónustuveitendur koma ekki til greina fyrir STEP.

Tafla yfir Þjónustuveitendur

Stig	Staðfestingargögn	Krafa
1	Árleg öryggismatsskýrsla um hlítingu á vettvangi	Skylda
2	Árlegur SAQ D (Þjónustuaðili) og Ársfjórðungsleg netkerfisskönnun eða Árleg öryggismatsskýrsla um hlítingu á vettvangi, ef þess er óskað	Skylda

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

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

Eftirfarandi gagna er krafist fyrir mismunandi stig Söluaðila og Þjónustuveitenda eins og kemur fram í Söluaðilatöflunni og Þjónustuveitendatöflunni að framan.

Árlegt öryggismat á vettvangi – Árlega skýrslan um öryggismat á vettvangi er nákvæm vettvangsskoðun á búnaði þínum, kerfum og netkerfum (og íhlutum þeirra) þar sem Korthafaupplýsingar eða Viðkvæm auðkenningargögn (eða bæði) eru geymd, unnið er úr þeim eða þau send. Hún skal framkvæmd af:

- QSA eða
- þér og vottuð af forstjóra þínum, fjármálastjóra, upplýsingaöryggisstjóra eða forsvarsmanni og send árlega til American Express á viðeigandi eyðublaði Vottunar á hlítingu (AOC).

AOC-eyðublaðið skal styðja við hlítingu á öllum kröfum PCI DSS-staðalsins og, sé þess óskað, innihalda afrit af allri skýrslunni um hlítingu (1. stigs Söluaðilar og 1. stigs Þjónustuveitendur).

Árlegur sjálfsmatsspurningalisti – Árlegur sjálfsmatsspurningalisti er ferli þar sem notast er við PCI DSS-SAQ sem gerir kleift að framkvæma nákvæma sjálfsskoðun á búnaði þínum, kerfum og netkerfum (og íhlutum þeirra) þar sem Korthafaupplýsingar eða Viðkvæm auðkenningargögn (eða bæði) eru geymd, unnið er úr þeim eða þau send. Hún verður að vera framkvæmd af þér og vottuð af framkvæmdastjóra þínum, fjármálastjóra, yfirmanni upplýsingaöryggis eða forsvarsmanni. Senda skal AOC-hluta SAQ árlega til American Express. AOC-hluti SAQ skal staðfesta að þú uppfyllir allar kröfur PCI DSS-staðalsins og innihalda afrit af öllum SAQ sé þess óskað (2. stigs, 3. stigs og 4. stigs Söluaðilar; 2. stigs Þjónustuveitendur).

Ársfjórðungsleg netskönnun – Ársfjórðungsleg netskönnun er ferli sem fjarprófar nettengd tölvukerfi og vefþjóna þína til að finna mögulega veikleika. Hún skal framkvæmd af Viðurkenndum skönnunaraðila (**ASV**). Þér ber að ljúka við og senda ASV-skönnunarskýrsluna um Vottun á skönnunarhlítingu (**AOSC**) eða samantekt á niðurstöðum skönnunarinnar (og afrit af allri skönnuninni, sé þess óskað) ársfjórðungslega til American Express. AOSC-skýrslan eða samantektin skal staðfesta að niðurstöðurnar séu í samræmi við skönnunarverklag PCI DSS-staðalsins, að engin áhættuatriði hafi fundist og að skönnunin hafi staðist og uppfylli kröfur (allir Söluaðilar nema þeir sem senda líka inn Skýrslu um öryggismat á vettvangi, Söluaðilar sem koma tilgreina fyrir STEP og allir Þjónustuveitendur). Til að forðast misskilning þá er Ársfjórðungsleg netkerfisskönnun tilskilin ef hennar er krafist af SAQ.

Árleg STEP-vottun – Árleg STEP-hæfisvottun American Express („STEP-vottun") er einungis í boði fyrir söluaðila sem uppfylla skilyrðin í Aðgerð 2: „Hafðu skilning á stigi þínu og Staðfestingarkröfum" að ofan. STEP-vottunin felur í sér ferli sem notar PCI DSS-kröfur sem gerir kleift sjálfsmat á búnaði þínum, kerfum og netkerfum (og íhlutum þeirra) þar sem Korthafaupplýsingar eða Viðkvæm auðkenningargögn (eða bæði) eru geymd, unnið úr þeim eða þau send. Hún verður að vera framkvæmd af þér og vottuð af framkvæmdastjóra þínum, fjármálastjóra, yfirmanni upplýsingaöryggis eða forsvarsmanni. Þú verður að klára ferlið með því að senda Staðfestingareyðublað fyrir STEP til American Express á hverju ári. (Aðeins Söluaðilar sem eru gjaldgengir fyrir STEP). Eyðublað fyrir Árlega STEP-vottun er fáanlegt til niðurhals í gegnum örugga vefgátt SecureTrust.

Ekki farið eftir PCI DSS – ef þú hlítir ekki PCI DSS þá verður þú að senda inn eitt af eftirfarandi skjölum:

- Staðfesting á hlítni (AOC) að meðtöldum „Hluta 4. Aðgerðaáætlun fyrir þá stöðu þegar misbrestur er á hlítni"
- PCI-forgangsnálgunartól fyrir samantekt og staðfestingu á hlítni (PASAOC)
- Sniðmát fyrir verkáætlun (fáanlegt til niðurhals í gegnum örugga vefgátt SecureTrust)

Til að hlítingu sé náð verður hvert af ofangreindum skjölum að tilgreina dagsetningu úrbóta, sem má ekki vera síðar en 12 mánuðum eftir að skjalið er sent. Þú verður að senda inn viðeigandi skjal til American Express samkvæmt einni af aðferðunum sem listaðar eru í Aðgerð 4: „Staðfestingargögn send til American Express" hér að neðan. Þú skalt upplýsa American Express með reglubundnum hætti um framgang úrbóta þinna vegna Misbrests á hlítni" (1. stigs, 2. stigs, 3. stigs og 4. stigs Söluaðilar; allir Þjónustuveitendur). Til að forðast misskilning þá koma Söluaðilar sem ekki hlíta PCI DSS ekki til greina fyrir STEP. American Express mun ekki krefja þig um ógildingargjöld (lýst að neðan) ef hlítingarstaða þín er neikvæð fyrir lokadagsetningu úrbóta, en þú ert áfram ábyrg(ur) gagnvart American Express vegna Gagnatilfella og ert bundin(n) öllum öðrum ákvæðum þessara reglna.

Aðgerð 4: Staðfestingargögn send til American Express

Allir Söluaðilar og Þjónustuveitendur sem verða að taka þátt í PCI-áætlun American Express varðandi hlítingu þurfa að senda inn þau Staðfestingargögn sem eru merkt „skylda" í töflunum í Aðgerð 2: „Hafðu skilning á stigi þínu og Staðfestingarkröfum". Þér ber að senda Staðfestingargögnin til SecureTrust með einni af eftirfarandi leiðum:

- **Örugg vefgátt**: Hægt er að senda Staðfestingargögn til SecureTrust í gegnum örugga vefgátt þeirra á https://portal.securetrust.com.

  Hafðu samband við SecureTrust með símanúmeri viðkomandi Lands eða með tölvupósti á americanexpresscompliance@securetrust.com til að fá leiðbeiningar um notkun vefgáttarinnar.
- **Öruggt fax**: Hægt er að faxa Staðfestingargögnin á faxnúmer: +1 (312) 276-4019. (+ er alþjóðlega forskeytið vegna beinna hringinga, alþjóðleg símagjöld gilda).

Vinsamlegast gefið upp nafn, viðskiptaheiti, nafn gagnaöryggistengiliðs, póstfang og símanúmer, og, fyrir Söluaðila eingöngu, 10 tölustafa American Express-söluaðilanúmer.

Ef almennar spurningar vakna um áætlunina eða ferlið hér að ofan skal hafa samband við SecureTrust í síma + 800 9000 1140 eða +1 (312) 267-3208 eða með tölvupósti á americanexpresscompliance@securetrust.com.

Lokið er við hlítingu og staðfestingu á þinn kostnað. Með því að senda Staðfestingargögn staðfestir þú við American Express að þér sé heimilt að birta upplýsingarnar sem þar koma fram og að þú afhendir American Express Staðfestingargögnin án þess að brjóta á rétti nokkurs annars aðila.

Markaðir	SecureTrust-símanúmer
Argentína	+ 800 9000 1140
Ástralía	+ 800 9000 1140
Austurríki	+ 800 9000 1140
Bandaríkin	1 866 659 9016
Bretland	+ 800 9000 1140
Búlgaría	+ 312 267 3208
Danmörk	+ 800 9000 1140
Eistland	+ 312 267 3208
Frakkland	+ 800 9000 1140
Grikkland	+ 312 267 3208
Holland	+ 312 267 3208
Hong Kong	+ 800 9000 1140
IDC	+ 888 900 0114
Indland	+ 000 800 100 1177
Írland	+ 800 9000 1140
Ísland	+ 800 9000 1140
Ítalía	+ 800 9000 1140
Japan	+ 312 267 3208
Kanada	1 866 659 9016
Króatía	+ 312 267 3208
Kýpur	+ 800 9000 1140
Lettland	+ 312 267 3208
Litháen	+ 312 267 3208
Malta	+ 312 267 3208

Markaðir	SecureTrust-símanúmer
Mexíkó	+ 888 900 0114
Noregur	+ 800 9000 1140
Nýja-Sjáland	+ 800 9000 1140
Pólland	+ 800 9000 1140
Portúgal	+ 312 267 3208
Rúmenía	+ 312 267 3208
Rússland	+ 312 267 3208
Singapúr	+ 800 9000 1140
Slóvakía	+ 312 267 3208
Slóvenía	+ 312 267 3208
Spánn	+ 800 9000 1140
Svíþjóð	+ 800 9000 1140
Taíland	+ 800 9000 1140
Taívan	+ 312 267 3208
Tékkland	+ 800 144 316
Ungverjaland	+ 800 9000 1140
Þýskaland	+ 800 9000 1140

+ er alþjóðlega forskeytið vegna beinna hringinga, alþjóðleg símagjöld gilda

Gjöld vegna misbrests á staðfestingu og uppsögn samnings

American Express er heimilt að innheimta af þér ógildingargjöld og segja upp Samningnum ef þú uppfyllir ekki þessar kröfur eða sendir ekki nauðsynleg Staðfestingargögn til American Express fyrir viðeigandi skilafrest. American Express mun láta þig vita hver viðeigandi skilafrestur er fyrir hvert árlegt og ársfjórðungslegt skýrslutímabil.

Sendu gögnin til American Express fyrir viðeigandi skilafrest. American Express mun láta þig vita hver viðeigandi skilafrestur er fyrir hvert árlegt og ársfjórðungslegt skýrslutímabil.

Tafla yfir ógildingargjöld

Lýsing*	Söluaðili á 1. stigi eða Þjónustuveitandi á 1. stigi	Söluaðili á 2. stigi eða Þjónustuveitandi á 2. stigi	Söluaðili á 3. eða 4. stigi
Ógildingargjald verður lagt á ef Staðfestingargögn berast ekki fyrir fyrsta skilafrest.	25.000$ Bandaríkjadalir	5.000$ Bandaríkjadalir	50$ Bandaríkjadalir
Aukalegt ógildingargjald verður lagt á ef Staðfestingargögn berast ekki innan 60 daga frá fyrsta skilafresti.	35.000$ Bandaríkjadalir	10.000$ Bandaríkjadalir	100$ Bandaríkjadalir
Aukalegt ógildingargjald verður lagt á ef Staðfestingargögn berast ekki innan 90 daga frá fyrsta skilafresti og á 30 daga fresti þar á eftir.	45.000$ Bandaríkjadalir	15.000$ Bandaríkjadalir	250$ Bandaríkjadalir

* Ógildingargjöld eru lögð á í Staðbundnum gjaldmiðli.

** Á ekki við í Argentínu.

Ef nauðsynleg Staðfestingargögn berast ekki American Express innan 90 daga frá fyrsta skilafresti er American Express heimilt að segja Samningnum upp í samræmi við ákvæði hans auk þess að innheimta af þér samanlögð ógildingargjöld.

Kafli 6 Þagnarskylda

American Express mun gera eðlilegar ráðstafanir til að gæta (og sjá til þess að umboðsmenn og undirverktakar sínir, þ.m.t. SecureTrust, gæti) trúnaðar um skýrslur þínar um hlítingu, þ.m.t. Staðfestingargögnin, og mun ekki birta staðfestingargögnin neinum þriðja aðila (öðrum en Hlutdeildarfélögum, 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 löggæsluyfirvalda).

Kafli 7 Fyrirvari

AMERICAN EXPRESS HAFNAR ALLRI ÁBYRGÐ OG BÓTASKYLDU Í TENGSLUM 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 ÞRIÐJU AÐILAR SEM NJÓTA RÉTTINDA SAMKVÆMT ÞESSUM REGLUM.

Gagnleg vefsvæði

Gagnaöryggi American Express: www.americanexpress.com/datasecurity

Öryggisstaðlaráð greiðslukortafyrirtækja, LLC: www.pcisecuritystandards.org

Orðalisti

Eftirfarandi skilgreiningar gilda um þessar Reglur um gagnaöryggi (DSOP) ef þær skarast á við hugtök sem koma fyrir í *Reglur fyrir söluaðila*.

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 2,5 milljónir American Express-kortafærslna á ári.

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

4. stigs Söluaðili er Söluaðili með minna 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 vinnur úr 2,5 milljónum eða færri American Express-kortafærslu á ári eða hver sá Þjónustuveitandi sem American Express telur ekki vera 1. stigs.

Aðilar undir ábyrgð á við um einhvern eða alla starfsmenn þína, umboðsmenn, fulltrúa, undirverktaka, Framkvæmdaaðila, Þjónustuveitendur, veitendur Posabúnaðar (POS) eða kerfa eða lausna við framkvæmd greiðsla, aðila sem tengjast þínum American Express-söluaðilareikningi og hverskyns aðra aðila sem þú veitt aðgang að Korthafaupplýsingum í samræmi við Samninginn.

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: EMV, Dulkóðun frá punkti til punkts og táknrgreining.

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 kortareikningsnúmer.

Áætlun um aukna öryggistækni (STEP) er áætlun American Express sem hvetur Söluaðila til að taka í notkun tækni sem eykur gagnaöryggi. Til að vera gjaldgengir í STEP má gagnatilvik ekki hafa komið upp hjá Söluaðila síðustu 12 mánuði fyrir innsendingu Árlegrar STEP-vottunar og a.m.k. 75% allra Færslna þeirra verða að vera gerðar með dulkóðun frá punkti til punkts eða Færslum augliti til auglitis með EMV-flögubúnaði.

Áætlun um miðaða greiningu er áætlun sem býður upp á skjóta greiningu mögulegs stulds á Korthafaupplýsingum í Gagnaumhverfi korthafa (CDE). Sjá Kafli 1, „Áætlun um miðaða greiningu (TAP)“.

BIP-færslur (Buyer Initiated Payments) eru Greiðslur sem gerðar eru með greiðslufyrirmælaskrá sem unnið er úr með BIP.

Dulkóðunarlykill („American Express dulkóðunarlykill“) er hver sá lykill sem notaður er við úrvinnslu, framleiðslu, hleðslu og/eða vörn eikningsgagna. Slíkir lyklar 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: Grunnafleiðslukyklar (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 fáanleg 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.

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 greiðsla eða kaup framkvæmd með Korti.

Færsla merkir Greiðsla eða Endurgreiðsla sem fór fram með Korti.

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

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 þín (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, skár 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.

Greiðsluumsókn hefur þá merkingu sem fram kemur í Orðalista fyrir öryggisstaðal greiðslukortafyrirtækja vegna greiðsluumsókna 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.

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

Korthafaupplýsingar hefur þá merkingu sem fram kemur í Orðalista fyrir PCI DSS-staðalinn sem í gildi er á hverjum tíma.

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.

Kröfur Öryggisstaðlaráðs 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.

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

PCI-rannsóknaraðili (PFI) er aðili sem hefur fengið samþykki Öryggisstaðlaráðs 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-öryggisstaðlaráðið, 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-viðskiptafærslna (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.

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 Öryggisstaðlaráði greiðslukortafyrirtækja, LLC, með það að markmiði að meta og votta hlítingu við PCI DSS.

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.

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

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

Tími sem gagnatilfelli varir er tímabilið frá dagsetningu stuldar, ef vitað er um hana, eða 365 dagar fyrir Dagsetningu tilkynningar ef ekki er vitað um dagsetningu stuldar. Tíma gagnatilfellis lýkur 30 dögum eftir Dagsetningu tilkynningar.

Tæki sem tekur við flögum 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.

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

Viðkvæm auðkenningargögn hefur þá merkingu sem fram kemur í Orðalista fyrir PCI DSS-staðalinn sem í gildi er á hverjum tíma.

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

Viðurkenndur skönnunaraðili (ASV) er Aðili sem hefur verið viðurkenndur af Öryggisstaðlaráði 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 Öryggisstaðlaráði greiðslukortafyrirtækja, LLC til að staðfesta hlítingu við PCI DSS-staðalinn.

Vottun á hlítingu (AOC) er yfirlýsing um stöðu hlítingar við PCI DSS-staðalinn á eyðublaði sem gefið er út af Öryggisstaðlaráði greiðslukortafyrirtækja, LLC.

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

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