

Data Security Operating Policy (DSOP)

Als toonaangevende onderneming op het gebied van consumentenbescherming legt American Express zich er reeds lang op toe Kaarthouderinformatie en Gevoelige verificatiegegevens te beschermen om ervoor te zorgen dat deze informatie vertrouwelijk bewaard wordt.

Gecompromitteerde gegevens hebben een negatieve invloed op consumenten, Kaartaccepterende bedrijven, Serviceproviders en kaartuitgevende bedrijven. Zelfs één incident kan de reputatie van een bedrijf ernstig schaden en het vermogen om effectief zaken te doen aantasten. Het beperken van dit risico door een beveiligingsbeleid te implementeren, kan het consumentenvertrouwen bevorderen, de winstgevendheid vergroten en de reputatie van een onderneming verbeteren.

American Express erkent dat onze Kaartaccepterende bedrijven en Serviceproviders (gezamenlijk **u**) onze zorgen delen en vereist als onderdeel van uw verantwoordelijkheden dat u voldoet aan de bepalingen over gegevensbeveiliging in uw overeenkomst om (in het geval van Kaartaccepterende bedrijven) of verwerking (in het geval van Serviceproviders) de American Express®-kaart te accepteren (respectievelijk de **Overeenkomst**) en deze *Data Security Operating Policy*, die we van tijd tot tijd kunnen wijzigen. Deze vereisten zijn van toepassing op al uw apparatuur, systemen en netwerken (en hun componenten) waarop Coderingssleutels, Kaarthouderinformatie of Gevoelige verificatiegegevens (of een combinatie daarvan) worden opgeslagen, verwerkt of verzonden.

De termen met een hoofdletter die hierin worden gebruikt maar niet worden gedefinieerd, hebben de betekenis die eraan wordt toegekend in de verklarende woordenlijst aan het einde van dit beleid.

Paragraaf 1 **Standaarden voor de bescherming van Coderingssleutels, Kaarthouderinformatie en Gevoelige verificatiegegevens**

U moet ervoor zorgen dat u en de partijen waar u mee werkt:

- Kaarthouderinformatie alleen opslaan om American Express-kaarttransacties mogelijk te maken conform en zoals vereist door de Overeenkomst.
- Voldoen aan de huidige PCI DSS- en andere PCI SSC-vereisten die van toepassing zijn op uw verwerking, opslag of verzending van Kaarthouderinformatie of Gevoelige verificatiegegevens en niet later dan de ingangsdatum van de implementatie van die versie van de toepasselijke vereiste.
- Op bemande locaties alleen door de PCI goedgekeurde nieuwe of vervangende Pinapparaten of Betaaltoepassingen (of beide) gebruiken.

U dient alle American Express-Betalingsoverzichten en kredietoverzichten te beschermen die conform de Overeenkomsten in overeenstemming met deze bepalingen betreffende beveiliging van gegevens worden aangereikt; u dient deze overzichten alleen te gebruiken voor doeleinden die in deze Overeenkomst aan de orde komen en deze op gepaste wijze te beveiligen. U bent financieel en anderszins aansprakelijk tegenover American Express om ervoor te zorgen dat uw Derde partijen deze bepalingen betreffende beveiliging van gegevens naleven (behalve om aan te tonen dat uw Derde partijen dit beleid naleven onder [Paragraaf 4, "Belangrijke periodieke validatie van uw systemen"](#), tenzij anders bepaald in die paragraaf).

Paragraaf 2 Verplichtingen omtrent beheer van Gegevensincidenten

U moet American Express onmiddellijk en in geen geval later dan vierentwintig (24) uur na ontdekking van een Gegevensincident op de hoogte stellen.

Neem contact op met het American Express Enterprise Incident Response Program (EIRP) om American Express op de hoogte te stellen op +1 (602) 537-3021 (+ geeft het internationale landnummer (IDD) aan, internationale belkosten zijn van toepassing), of stuur een e-mail naar EIRP@aexp.com. U moet een persoon aanwijzen als uw contactpersoon met betrekking tot een dergelijk Gegevensincident. Bovendien:

- Moet u voor elk Gegevensincident een grondig forensisch onderzoek uitvoeren.
- Voor Gegevensincidenten waarbij 10.000 of meer unieke kaartnummers betrokken zijn, moet u binnen vijf (5) dagen na ontdekking van een Gegevensincident een PCI Forensic Investigator (PFI) inschakelen om dit onderzoek uit te voeren.
- Het onbewerkte forensisch onderzoeksrapport moet binnen tien (10) werkdagen na voltooiing aan American Express worden verstrekt.
- Moet u American Express onmiddellijk alle gecompromitteerde kaartnummers verstrekken. American Express behoudt zich het recht voor om zijn eigen interne analyse uit te voeren om kaartnummers te identificeren die bij het Gegevensincident zijn betrokken.

Forensische onderzoeksrapporten moeten worden ingevuld met behulp van de huidige Forensic Incident Final Report Template die verkrijgbaar is bij PCI. Dit rapport moet forensische beoordelingen, rapportages over naleving en alle andere informatie over het Gegevensincident bevatten; de oorzaak van het Gegevensincident identificeren; bevestigen of u al dan niet in overeenstemming was met de PCI DSS op het moment van het Gegevensincident; en uw vermogen verifiëren om toekomstige Gegevensincidenten te voorkomen door (i) een plan te verstrekken om alle tekortkomingen op het vlak van PCI DSS te verhelpen, en (ii) deel te nemen aan het nalevingsprogramma van American Express (zoals hieronder beschreven). Op verzoek van American Express moet u een validatie door een Qualified Security Assessor (QSA) aanleveren, om aan te tonen dat de tekortkomingen zijn verholpen.

Ondanks de voorgaande paragrafen in deze [Paragraaf 2, "Verplichtingen omtrent beheer van Gegevensincidenten"](#):

- Kan American Express naar eigen goeddunken van u eisen dat u een PFI inschakelt om een onderzoek uit te voeren naar een Gegevensincident, waarbij minder dan 10.000 unieke kaartnummers zijn betrokken. Een dergelijk onderzoek moet voldoen aan de vereisten die hierboven in deze [Paragraaf 2, "Verplichtingen omtrent beheer van Gegevensincidenten"](#) zijn uiteengezet en moet binnen de door American Express vereiste periode worden voltooid.
- Kan American Express naar eigen goeddunken afzonderlijk een PFI inschakelen om een onderzoek uit te voeren naar een Gegevensincident en de kosten van een dergelijk onderzoek bij u in rekening brengen.

U stemt ermee in om met American Express samen te werken om eventuele problemen die voortvloeien uit het Gegevensincident op te lossen, waaronder overleg met American Express over uw communicatie met Kaarthouders die door het Gegevensincident zijn getroffen. Ook dient u American Express alle relevante informatie te verstrekken (en eventuele ontheffingen op de verstrekking te verkrijgen), om te verifiëren dat u toekomstige Gegevensincidenten kunt voorkomen op een wijze die in overeenstemming is met deze Overeenkomst.

Ondanks eventuele tegengestelde geheimhoudingsverplichtingen in de Overeenkomst, heeft American Express het recht om informatie over Gegevensincidenten bekend te maken aan American Express-Kaarthouders, Kaartuitgevende bedrijven, andere deelnemers aan het American Express-netwerk en het algemene publiek, indien vereist door de toepasselijke wetgeving. Dit gebeurt door gerechtelijk, administratief of regelgevend bevel, decreet, dagvaarding, verzoek of ander proces, om het risico op fraude of andere schade te beperken, of anderszins voor zover passend om het American Express-netwerk te exploiteren.

Paragraaf 3 Schadeloosstellingsverplichtingen voor een Gegevensincident

Uw schadeloosstellingsverplichtingen aan American Express onder de Overeenkomst voor Gegevensincidenten worden bepaald, zonder afstand te doen van eventuele andere rechten en rechtsmiddelen van American Express, in deze [Paragraaf 3, "Schadeloosstellingsverplichtingen voor een Gegevensincident"](#). Naast uw schadeloosstellingsverplichtingen (indien van toepassing), kunt u onderworpen zijn aan een vergoeding voor niet-naleving van Gegevensincidenten, zoals hieronder beschreven in deze [Paragraaf 3, "Schadeloosstellingsverplichtingen voor een Gegevensincident"](#).

Voor Gegevensincidenten waarbij sprake is van:

- 10.000 of meer American Express-kaartnummers met een van de volgende kenmerken:
 - Gevoelige verificatiegegevens of
 - Vervaldatum
- betaalt u American Express een vergoeding van \$ 5 USD per rekeningnummer.

American Express zal echter geen schadevergoeding van u verlangen voor een Gegevensincident dat betrekking heeft op:

- minder dan 10.000 American Express-kaartnummers of
- meer dan 10.000 American Express-kaartnummers, als u aan de volgende voorwaarden voldoet:
 - u heeft American Express op de hoogte gebracht van het Gegevensincident op grond van [Paragraaf 3, "Schadeloosstellingsverplichtingen voor een Gegevensincident"](#),
 - u voldeed op het moment van het Gegevensincident aan de PCI DSS (zoals bepaald door het onderzoek van de PFI naar het Gegevensincident), en
 - het Gegevensincident is niet veroorzaakt door foutief handelen van u of uw Derde partijen.

Niettegenstaande de voorgaande paragrafen in deze [Paragraaf 3, "Schadeloosstellingsverplichtingen voor een Gegevensincident"](#) voor elk Gegevensincident, ongeacht het aantal American Express-kaartnummers, betaalt u American Express een boete voor niet-naleving met betrekking tot Gegevensincidenten van maximaal \$ 100.000 USD per Gegevensincident (zoals bepaald door American Express en naar eigen goeddunken), indien u niet voldoet aan uw verplichtingen, zoals uiteengezet in [Paragraaf 2, "Verplichtingen omtrent beheer van Gegevensincidenten"](#). Voor alle duidelijkheid: de totale boete voor niet-naleving met betrekking tot Gegevensincidenten die voor een enkel Gegevensincident worden berekend, zal niet hoger zijn dan \$ 100.000 USD.

American Express zal van zijn berekening elk American Express-kaartrekeningnummer uitsluiten dat is betrokken bij een eerdere schadeloosstellingsvordering bij een Gegevensincident die binnen twaalf (12) maanden voorafgaand aan de Notificatiedatum is gedaan. Alle berekeningen die door American Express volgens deze methodologie zijn gemaakt, zijn definitief.

American Express kan u volgens de Overeenkomst het volledige bedrag van uw schadeloosstellingsverplichting voor Gegevensincidenten in rekening brengen of het bedrag aftrekken van de betalingen van American Express aan u (of uw bankrekening dienovereenkomstig debiteren).

De schadeloosstellingsverplichting voor Kaartaccepterende bedrijven in geval van Gegevensincidenten zullen niet worden beschouwd als incidentele, indirecte, speculatieve, gevolg-, speciale, punitieve of voorbeeldschade onder deze Overeenkomst, op voorwaarde dat een dergelijke verplichting geen schade omvat die verband houdt met of in de vorm is van gederfde winst of inkomsten, verlies van goodwill of verlies van zakelijke kansen.

American Express kan naar eigen goeddunken de schadeloosstellingsverplichting voor Kaartaccepterende bedrijven beperken, echter uitsluitend voor Gegevensincidenten die aan elk van de volgende criteria voldoen:

- Er werden toepasselijke Preventieve technologieën voorafgaand aan het Gegevensincident toegepast en deze waren tijdens de gehele Gegevensincidentperiode in gebruik,
- Een gedegen onderzoek conform het PFI-programma is afgerond (tenzij vooraf schriftelijk anders is overeengekomen),

- Het forensisch rapport vermeldt duidelijk dat Preventieve technologieën werden gebruikt om de gegevens te verwerken, op te slaan en/of te verzenden op het moment van het Gegevensincident, en
- U slaat/sloeg geen Gevoelige verificatiegegevens of Kaarthouderinformatie op die niet onleesbaar zijn/waren gemaakt (en bewaart/bewaarde deze ook niet tijdens de gehele Gegevensincidentperiode).

Als een schadeloosstellingsvermindering beschikbaar is, wordt de vermindering van uw schadeloosstellingsverplichting (met uitzondering van eventuele te betalen boetes voor niet-naleving) als volgt bepaald:

Verlaging van de schadeloosstellingsverplichting	Vereiste criteria
Standaardverlaging: 50%	>75% van de totale transacties op apparaten met een chipfunctie ¹ OF Preventieve technologie in gebruik op >75% van Kaartaccepterende bedrijfslocaties ²
Extra verlaging: 75% tot 100%	>75% van alle transacties op apparaten met een chipfunctie ¹ EN andere Preventieve technologie in gebruik in minimaal >75% van Kaartaccepterende bedrijfslocaties ²

¹ Zoals vastgesteld door interne analyse door American Express

² Zoals vastgesteld door een onderzoek van de PFI

- De Extra verlaging (75% tot 100%) zal worden vastgesteld op basis van het percentage transacties op apparaten met een chipfunctie OF, indien lager, Kaartaccepterende bedrijfslocaties die een andere Preventieve technologie gebruiken. Onderstaande voorbeelden illustreren de berekening van de schadeloosstellingsvermindering.
- Om te worden beschouwd als een Preventieve technologie, moet u aantonen dat de technologie effectief wordt gebruikt in overeenstemming met het ontwerp en het beoogde doel. De installatie van apparaten met een chipfunctie en de verwerking van chipkaarten als transacties met een magnetische strip of een invoercode zijn GEEN voorbeelden van een effectieve toepassing van deze technologie.
- Het percentage locaties dat een Preventieve technologie gebruikt, wordt bepaald door onderzoek van de PFI.
- De vermindering van de schadeloosstellingsverplichting is niet van toepassing op eventuele boetes voor niet-naleving die verschuldigd zijn in verband met het Gegevensincident.

Bv.	Preventieve technologie in gebruik	Komt u in aanmerking voor een extra verlaging van de schadeloosstellingsverplichting?	Verlaging
1	80% van alle transacties op apparaten met een chipfunctie	Nee	50%: Standaardverlaging (minder dan 75% gebruik van Preventieve technologie kwalificeert niet voor een Extra verlaging) ¹
	0% van de locaties gebruikt andere Preventieve technologie		
2	80% van de transacties op apparaten met een chipfunctie	Ja	77%: Extra verlaging (gebaseerd op 77% Preventieve technologie in gebruik)
	77% van de locaties gebruikt andere Preventieve technologie		

Bv.	Preventieve technologie in gebruik	Komt u in aanmerking voor een extra verlaging van de schadeloosstellingsverplichting?	Verlaging
3	93% van de transacties op apparaten met een chipfunctie	Ja	93%: Extra verlaging (gebaseerd op 93% van de transacties op apparaten met een chipfunctie)
	100% van de locaties gebruikt andere Preventieve technologie		
4	40% van de transacties op apparaten met een chipfunctie	Nee	50%: Standaardverlaging (minder dan 75% transacties op apparaten met een chipfunctie kwalificeert niet voor Extra verlaging)
	90% van de locaties gebruikt andere Preventieve technologie		

¹ Een Gegevensincident waarbij 10.000 American Express Card-rekeningen betrokken zijn, tegen een tarief van \$ 5 USD per rekeningnummer (10.000 x \$ 5 = \$ 50.000 USD) kan in aanmerking komen voor een vermindering van 50%, waardoor de schadeloosstellingsverplichtingen worden verlaagd van \$ 50.000 USD naar \$ 25.000 USD, exclusief boetes voor niet-naleving.

Paragraaf 4 Belangrijke periodieke validatie van uw systemen

U moet, zoals hieronder beschreven, jaarlijks en driemaandelijks de volgende PCI DSS-acties ondernemen om de status te valideren van de apparatuur, systemen en/of netwerken (en hun componenten) van u en uw franchisenemers waarop Kaarthouderinformatie of Gevoelige verificatiegegevens worden opgeslagen, verwerkt of verzonden.

Er zijn vier acties vereist om aan validatie te voldoen:

[Actie 1:](#) Deelnemen aan het nalevingsprogramma van American Express conform dit beleid.

[Actie 2:](#) Uw niveau en valideringsvereisten begrijpen.

[Actie 3:](#) De Valideringsdocumentatie invullen die u dient te verzenden naar American Express.

[Actie 4:](#) De Valideringsdocumentatie verzenden naar American Express binnen de voorgeschreven deadlines.

Actie 1: Deelnemen aan het nalevingsprogramma van American Express conform dit beleid.

Kaartaccepterende bedrijven van niveau 1, Kaartaccepterende bedrijven van niveau 2 en alle Serviceproviders zoals hieronder beschreven, moeten deelnemen aan het PCI-nalevingsprogramma van American Express onder dit beleid door de volledige naam, het e-mailadres, telefoonnummer en het fysieke postadres op te geven van degene die als algemeen contactpersoon voor gegevensbeveiliging optreedt. U moet deze informatie verzenden naar SecureTrust, een divisie van Trustwave (<https://portal.securetrust.com>), die het programma beheert namens American Express, door een van de methoden vermeld in [Actie 4: "De Valideringsdocumentatie verzenden naar American Express"](#) hieronder. U moet SecureTrust op de hoogte stellen als deze informatie verandert en de bijgewerkte gegevens aanleveren, als dit van toepassing is. Als u dergelijke contactgegevens niet verstrekt, heeft dit geen invloed op onze rechten om een boete voor niet valideren te beoordelen, zoals uiteengezet in de [Tabel Boetes voor niet valideren](#).

American Express kan naar eigen goeddunken de deelname van bepaalde Kaartaccepterende bedrijven van niveau 3 en niveau 4 aan het nalevingsprogramma van American Express onder dit beleid toewijzen door hen schriftelijk op de hoogte te stellen. Het Kaartaccepterend bedrijf moet zich uiterlijk 90 dagen na ontvangst van de notificatie aanmelden.

Actie 2: Uw niveau en valideringsvereisten begrijpen

Er zijn vier niveaus die van toepassing zijn op Kaartaccepterende bedrijven en twee niveaus op Serviceproviders op basis van uw aantal American Express-kaarttransacties. Voor Kaartaccepterende bedrijven is dit het door hun vestigingen ingediende volume dat doorloopt naar het hoogste American Express accountniveau voor Kaartaccepterende bedrijven.* U valt in een van de niveaus die zijn gespecificeerd in de onderstaande tabellen voor Kaartaccepterende bedrijven en Serviceproviders. Buyer Initiated Payments-betalingen (BIP) zijn niet inbegrepen in het volume van American Express-kaarttransacties om het niveau van het Kaartaccepterende bedrijf en de valideringsvereisten te bepalen.

* In het geval van franchisegevers omvat dit het aantal van de vestigingen van hun franchisenemers. Franchisegevers die opleggen dat franchisenemers een gespecificeerd Point of Sale-systeem (POS-systeem) of gespecificeerde Serviceprovider gebruiken, dienen ook Valideringsdocumentatie te verstrekken voor de betreffende franchisenemers.

Verplichtingen van Kaartaccepterende bedrijven

Kaartaccepterende bedrijven (geen Serviceproviders) hebben vier mogelijke classificaties met betrekking tot hun niveau en valideringsvereisten. Nadat u het niveau van het Kaartaccepterende bedrijf uit de onderstaande lijst hebt bepaald, raadpleegt u de Tabel voor Kaartaccepterende bedrijven om de vereisten voor Valideringsdocumentatie te bepalen.

- **Kaartaccepterende bedrijven van niveau 1** – 2,5 miljoen American Express-kaarttransacties of meer per jaar, of elk Kaartaccepterend bedrijf dat anderszins en naar eigen goeddunken volgens American Express onder niveau 1 valt.
- **Kaartaccepterende bedrijven van niveau 2** – 50.000 tot 2,5 miljoen American Express-kaarttransacties per jaar.
- **Kaartaccepterende bedrijven van niveau 3** – 10.000 tot 50.000 American Express-kaarttransacties per jaar.
- **Kaartaccepterende bedrijven van niveau 4** – Minder dan 10.000 American Express-kaarttransacties per jaar.

Tabel voor Kaartaccepterende bedrijven

	Valideringsdocumentatie		
Niveau van Kaartaccepterend bedrijf/Jaarlijkse American Express-transacties	Nalevingsrapport (ROC) voor beoordeling ter plaatse	Enquête voor zelfbeoordeling (SAQ) EN driemaandelijke netwerkscan	STEP-attest voor in aanmerking komende Kaartaccepterende bedrijven
Niveau 1/ 2,5 miljoen of meer	Verplicht	Niet van toepassing	Optioneel (vervangt ROC)
Niveau 2/ 50.000 tot 2,5 miljoen	Optioneel	SAQ verplicht (tenzij een beoordeling op locatie wordt ingediend); scan verplicht bij bepaalde SAQ-typen	Optioneel (vervangt SAQ en netwerkscan of ROC)
Niveau 3/ 10.000 tot 50.000	Optioneel	SAQ optioneel (verplicht indien vereist door American Express); scan verplicht met bepaalde SAQ-typen	Optioneel (vervangt SAQ en netwerkscan of ROC)
Niveau 4/ 10.000 of minder	Optioneel	SAQ optioneel (verplicht indien vereist door American Express); scan verplicht met bepaalde SAQ-typen	Optioneel (vervangt SAQ en netwerkscan of ROC)

* Voor alle duidelijkheid: Kaartaccepterende bedrijven van niveau 3 en niveau 4 hoeven geen Valideringsdocumentatie in te dienen, tenzij dit naar goeddunken van American Express vereist is, maar zij moeten toch voldoen aan en zijn onderworpen aan aansprakelijkheid onder alle andere bepalingen van deze Data Security Operating Policy.

American Express behoudt zich het recht voor om de juistheid en geschiktheid van de verstrekte PCI-Valideringsdocumentatie te controleren, inclusief door op kosten van American Express een QSA of PFI van onze keuze in te schakelen.

Programma voor verbeteringen van beveiligingstechnologie (STEP)

Kaartaccepterende bedrijven die aan PCI DSS voldoen, kunnen naar goeddunken van American Express ook in aanmerking komen voor het STEP-programma van American Express als ze bepaalde aanvullende beveiligingstechnologieën in hun kaartverwerkende omgeving implementeren. STEP is alleen van toepassing als het Kaartaccepterend bedrijf in de afgelopen 12 maanden geen Gegevensincident heeft meegemaakt en als 75% van alle kaarttransacties van het Kaartaccepterend bedrijf wordt uitgevoerd met behulp van:

- **EMV** – op een actief chipapparaat met een geldige en actuele EMVCo-goedkeuring/-certificering (www.emvco.com) dat voor AEIPS geschikte transacties met Chipkaarten kan verwerken. (Amerikaanse Kaartaccepterende bedrijven dienen ook contactloos te gebruiken)
- **Point-to-Point-codering (P2PE)** – gecommuniceerd naar de processor van het Kaartaccepterende bedrijf met behulp van een door de PCI-SSC of QSA goedgekeurd point-to-point-coderingssysteem

Voor Kaartaccepterende bedrijven die in aanmerking komen voor STEP zijn verlaagde vereisten voor te valideren PCI-documentatie van toepassing, zoals hieronder beschreven in [Actie 3: "De Valideringsdocumentatie invullen die u dient te verzenden naar American Express"](#) hieronder.

Vereisten voor Serviceproviders

Serviceproviders (geen Kaartaccepterende bedrijven) hebben twee mogelijke classificaties met betrekking tot hun niveau en valideringsvereisten. Nadat u het niveau van de Serviceprovider uit de onderstaande lijst hebt bepaald, raadpleegt u de Tabel voor Serviceproviders om de vereisten voor Valideringsdocumentatie te bepalen.

Serviceprovider van niveau 1 – 2,5 miljoen American Express-kaarttransacties of meer per jaar, of een Serviceprovider die anderszins door American Express als niveau 1 wordt beschouwd.

Serviceprovider van niveau 2 – minder dan 2,5 miljoen American Express-kaarttransacties per jaar, of een Serviceprovider die door American Express niet als niveau 1 wordt beschouwd.

Serviceproviders komen niet in aanmerking voor STEP.

Tabel voor Serviceproviders

Niveau	Valideringsdocumentatie	Vereiste
1	Jaarlijks rapport van beveiligingstoetsing op locatie	Verplicht
2	Jaarlijkse SAQ D (Serviceprovider) en driemaandelijke netwerkscan of jaarlijks rapport van beveiligingstoetsing op locatie, indien gewenst.	Verplicht

Het wordt aanbevolen dat Serviceproviders ook voldoen aan de aanvullende PCI-validering voor aangewezen entiteiten.

Actie 3: De Valideringsdocumentatie invullen die u dient te verzenden naar American Express

De volgende documenten zijn vereist voor verschillende niveaus van Kaartaccepterende bedrijven en Serviceproviders, zoals vermeld in de bovenstaande Tabel voor Kaartaccepterende bedrijven en Tabel voor Serviceproviders.

Jaarlijkse beveiligingstoetsing op locatie – De jaarlijkse beveiligingstoetsing op locatie is een gedetailleerd onderzoek ter plaatse van uw apparatuur, systemen en netwerken (en hun componenten) waar Kaarthouderinformatie of Gevoelige verificatiegegevens (of beide) worden opgeslagen, verwerkt of verzonden. Deze toetsing moet worden uitgevoerd door:

- een QSA of
- door u en bevestigd door uw chief executive officer, chief financial officer, chief information security officer of directeur en jaarlijks worden ingediend bij American Express op basis van het toepasselijke Attest van naleving (AOC).

Het AOC moet de naleving aantonen van alle vereisten van de PCI DSS en op verzoek kopieën bijvoegen van het volledige nalevingsrapport (Kaartaccepterende bedrijven van niveau 1 en Serviceproviders van niveau 1).

Jaarlijkse Enquête voor zelfbeoordeling – De jaarlijkse zelfbeoordeling is een proces waarbij gebruik wordt gemaakt van de PCI DSS SAQ waarmee u uw apparatuur, systemen en netwerken (en hun componenten) zelf kunt onderzoeken waarin Kaarthouderinformatie of Gevoelige verificatiegegevens (of beide) worden opgeslagen, verwerkt of verzonden. Dit moet door u worden uitgevoerd en worden bevestigd door uw chief executive officer, chief financial officer, chief information security officer of directeur. Het AOC-onderdeel van de SAQ moet jaarlijks worden ingediend bij American Express. Het AOC-onderdeel van de SAQ moet bevestigen dat u aan alle vereisten van de PCI DSS voldoet en op verzoek volledige exemplaren van de SAQ omvatten (Kaartaccepterende bedrijven van niveau 2, 3 en 4 en Serviceproviders van niveau 2).

Driemaandelijke netwerkscan – De driemaandelijke netwerkscan is een proces dat uw op internet aangesloten computernetwerken en webserver op afstand test op mogelijke zwakheden en kwetsbaarheden. Dit moet worden uitgevoerd door een goedgekeurde scanprovider (**ASV**). U dient elk kwartaal het Scanrapport met attest van nakoming van scanregels van de ASV (**AOSC**) of de executive summary van de bevindingen van de scan (en op aanvraag kopieën van de volledige scan) te voltooien en in te dienen bij American Express. Uit de AOSC of executive summary dient te blijken dat de resultaten voldoen aan de PCI DSS-scanprocedures, dat er geen grote risico's zijn geïdentificeerd en dat de scan voldoet aan de regels (alle Kaartaccepterende bedrijven, behalve degenen die ook een rapport van beveiligingstoetsing op locatie indienen, Kaartaccepterende bedrijven die voor STEP in aanmerking komen, en alle Serviceproviders). Voor alle duidelijkheid: driemaandelijke netwerkscans zijn verplicht indien vereist door de toepasselijke SAQ.

Valideringsdocumentatie voor het jaarlijkse STEP-attest – Het jaarlijkse STEP-kwalificatieattest van American Express ('STEP-attest') is alleen beschikbaar voor Kaartaccepterende bedrijven die voldoen aan de criteria in [Actie 2: "Uw niveau en valideringsvereisten begrijpen"](#) hierboven. Het STEP-attest omvat een proces dat gebruikmaakt van PCI DSS-vereisten waarmee zelfonderzoek van uw apparatuur, systemen en netwerken (en hun componenten) mogelijk is waar Kaarthouderinformatie of Gevoelige verificatiegegevens (of beide) worden opgeslagen, verwerkt of verzonden. Dit moet door u worden uitgevoerd en worden bevestigd door uw CEO, CFO, CISO of Principal Officer. U moet het proces voltooien door het STEP-attestformulier jaarlijks bij American Express in te dienen. (Alleen Kaartaccepterende bedrijven die in aanmerking komen voor STEP). Het jaarlijkse STEP-attestformulier is online te downloaden via de veilige portal van SecureTrust.

Samenvatting van naleving (SOC) – De samenvatting van naleving (SOC) is een document waarmee een franchisegever of Serviceprovider de PCI-nalevingsstatus van zijn franchisenemers kan rapporteren. Het SOC-sjabloon kan worden gedownload via de veilige portal van SecureTrust.

Niet-naleving van PCI DSS – Als u niet voldoet aan de PCI DSS, moet u een van de volgende documenten overleggen:

- Attest van naleving (AOC), inclusief 'Deel 4. Actieplan in geval van niet-naleving'
- een Geprioriteerde aanpaksummarie en Attest van naleving van de PCI DSS (PASAOC)
- een projectplansjabloon (kan worden gedownload via de veilige portal van SecureTrust)

In elk van de bovenstaande documenten dient u aan te geven op welke datum het probleem is verholpen. Deze datum dient voor succesvolle naleving binnen 12 maanden van de datum van het document te liggen. U moet het juiste document bij American Express indienen via een van de methoden die worden vermeld in [Actie 4: "De Valideringsdocumentatie verzenden naar American Express"](#) hieronder. U dient American Express periodiek op de hoogte te houden van uw voortgang in het herstel van uw niet-conforme status (Kaartaccepterende bedrijven van niveau 1, 2, 3 en 4; alle Serviceproviders). Voor alle duidelijkheid, Kaartaccepterende bedrijven die niet voldoen aan PCI DSS komen niet in aanmerking voor STEP. American Express zal u voorafgaand aan de hersteldatum geen boetes voor niet valideren (hieronder beschreven) opleggen voor niet-naleving, maar u blijft aansprakelijk tegenover American Express voor alle schadeloosstellingsverplichtingen voor een Gegevensincident en onderworpen aan alle andere bepalingen van dit beleid.

Actie 4: De Valideringsdocumentatie verzenden naar American Express

Alle Kaartaccepterende bedrijven en Serviceproviders die verplicht deelnemen aan het American Express PCI-nalevingsprogramma moeten de Valideringsdocumentatie indienen die als 'verplicht' is gemarkeerd in de tabellen in [Actie 2: "Uw niveau en valideringsvereisten begrijpen"](#). U moet uw Valideringsdocumentatie verzenden aan SecureTrust via een van de volgende methoden:

- **Veilige portal:** Valideringsdocumentatie kan worden geüpload via de veilige portal van SecureTrust op <https://portal.securetrust.com>.
Neem contact op met SecureTrust via het telefoonnummer van uw land of stuur een e-mail naar americanexpresscompliance@securetrust.com voor de gebruikshandleiding voor deze portal.
- **Veilige fax:** Valideringsdocumentatie kan worden gefaxt naar fax naar +1 (312) 276-4019. (+ geeft de landcode aan voor internationaal telefoonverkeer (IDD), internationale belkosten zijn van toepassing).
Vermeld uw naam, bedrijfsnaam (DBA - Doing Business As), de naam van uw contactpersoon voor gegevensbeveiliging, uw adres en telefoonnummer en, alleen voor Kaartaccepterende bedrijven, uw tiencijferige American Express Kaartaccepterende bedrijven-aansluitnummer.

Neem als u vragen heeft over het bovenstaande programma of proces contact op met SecureTrust via + 800 9000 1140 of +1 (312) 267-3208 of via e-mail op americanexpresscompliance@securetrust.com.

Naleving en validering worden op uw kosten voltooid. Door uw Valideringsdocumentatie in te dienen, verklaart en garandeert u American Express dat u gemachtigd bent om de informatie daarin vrij te geven en de Valideringsdocumentatie aan American Express te verstrekken zonder de rechten van een andere partij te schenden.

Markten	SecureTrust Telefoonnummer
Argentinië	+ 800 9000 1140
Australië	+ 800 9000 1140
Bulgarije	+ 312 267 3208
Canada	1 866 659 9016
Cyprus	+ 800 9000 1140
Denemarken	+ 800 9000 1140
Duitsland	+ 800 9000 1140
Estland	+ 312 267 3208
Frankrijk	+ 800 9000 1140
Griekenland	+ 312 267 3208
Hongarije	+ 800 9000 1140
Hongkong	+ 800 9000 1140
IDC	+ 888 900 0114
Ierland	+ 800 9000 1140
IJsland	+ 800 9000 1140
India	+ 800 9000 1140
Italië	+ 800 9000 1140
Japan	+ 312 267 3208
Kroatië	+ 312 267 3208
Letland	+ 312 267 3208
Litouwen	+ 312 267 3208

Markten	SecureTrust Telefoonnummer
Malta	+ 312 267 3208
Mexico	+ 888 900 0114
Nederland	+ 312 267 3208
Nieuw-Zeeland	+ 800 9000 1140
Noorwegen	+ 800 9000 1140
Oostenrijk	+ 800 9000 1140
Polen	+ 800 9000 1140
Portugal	+ 312 267 3208
Roemenië	+ 312 267 3208
Rusland	+ 312 267 3208
Singapore	+ 800 9000 1140
Slovenië	+ 312 267 3208
Slowakije	+ 312 267 3208
Spanje	+ 800 9000 1140
Taiwan	+ 312 267 3208
Thailand	+ 800 9000 1140
Tsjechië	+ 800 144 316
Verenigd Koninkrijk	+ 800 9000 1140
Verenigde Staten	1 866 659 9016
Zweden	+ 800 9000 1140

+ geeft de landcode aan voor internationaal telefoonverkeer (IDD), internationale belkosten zijn van toepassing

Boetes voor niet valideren en beëindiging van de Overeenkomst

American Express heeft het recht om een boete voor niet valideren aan u op te leggen en de Overeenkomst te beëindigen als u niet aan deze vereisten voldoet of de verplichte Valideringsdocumentatie niet binnen de toepasselijke deadline aan American Express verstrekt. American Express zal u voor elke jaarlijkse en driemaandelijke rapportageperiode afzonderlijk informeren over de toepasselijke deadline.

Stuur de documentatie vóór de toepasselijke deadline naar American Express. American Express zal u voor elke jaarlijkse en driemaandelijke rapportageperiode afzonderlijk informeren over de toepasselijke deadline. Zie hieronder de Tabel Boetes voor niet valideren voor boetes die van toepassing zijn op uw land.

Beschrijving	Kaartaccepterend bedrijf van niveau 1 of Serviceprovider van niveau 1	Kaartaccepterend bedrijf van niveau 2 of Serviceprovider van niveau 2 of STEP-Kaartaccepterend bedrijf	Kaartaccepterend bedrijf van niveau 3 of niveau 4
Indien de Valideringsdocumentatie niet voor de eerste deadline is ontvangen, wordt een boete voor niet valideren in rekening gebracht.	Boete eerste maand voor niveau 1	Boete eerste maand voor niveau 2	Boete per maand
Er wordt een extra boete voor niet valideren bepaald als de Valideringsdocumentatie niet binnen 30 dagen na de eerste deadline is ontvangen.	Boete tweede maand voor niveau 1	Boete tweede maand voor niveau 2	
Er wordt een extra boete voor niet valideren bepaald als de Valideringsdocumentatie niet binnen 60 dagen na de eerste deadline is ontvangen.	Boete derde maand voor niveau 1	Boete derde maand voor niveau 3	

Als American Express uw verplichte Valideringsdocumentatie niet binnen 60 dagen na de eerste deadline heeft ontvangen, heeft American Express het recht om de Overeenkomst te beëindigen in overeenstemming met de voorwaarden en de bovenstaande boetes voor niet valideren cumulatief aan u op te leggen.

Tabel Boetes voor niet valideren

Markt	Niveau	Type	Valuta	Boete eerste maand	Boete tweede maand	Boete derde maand
Australië	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	AUD	35.000	49.000	63.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	AUD	7.000	14.000	21.000
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	AUD	Boete per maand: 20		
Bulgarije	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	BGN	28.000	40.000	51.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	BGN	5.500	11.000	16.500
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	BGN	Boete per maand: 33		

Markt	Niveau	Type	Valuta	Boete eerste maand	Boete tweede maand	Boete derde maand
Kroatië	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	HRK	105.000	152.000	195.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	HRK	21.000	42.000	63.000
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	HRK	Boete per maand: 130		
Cyprus, Estland, Frankrijk, Duitsland, Ierland, Spanje, Letland, Litouwen, Portugal, Slowakije, Slovenië	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	EUR	19.000	26.000	34.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	EUR	4.000	7.500	11.000
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	EUR	Boete per maand: 15		
Tsjechië	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	CZK	392.000	564.000	721.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	CZK	78.300	157.000	235.000
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	CZK	Boete per maand: 440		
Denemarken	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	DKK	110.000	156.000	200.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	DKK	22.000	42.000	65.000
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	DKK	Boete per maand: 130		
Hongkong	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	HKD	25.000	35.000	45.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	HKD	5.000	10.000	15.000
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	HKD	Boete per maand: 150		

Markt	Niveau	Type	Valuta	Boete eerste maand	Boete tweede maand	Boete derde maand
Hongarije	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	HUF	4.650.000	6.700.000	8.600.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	HUF	930.000	1.860.000	2.800.000
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	HUF	Boete per maand: 5.500		
IJsland	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	ISK	3.070.000	4.300.000	5.500.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	ISK	615.000	920.000	1.227.200
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	ISK	Boete per maand: 2.400		
Nieuw-Zeeland	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	NZD	35.000	49.000	63.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	NZD	7.000	14.000	21.000
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	NZD	Boete per maand: 20		
Noorwegen	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	NOK	135.000	195.000	249.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	NOK	27.000	54.000	81.000
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	NOK	Boete per maand: 170		

Markt	Niveau	Type	Valuta	Boete eerste maand	Boete tweede maand	Boete derde maand
Singapore	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	SGD	38.000	53.000	68.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	SGD	7.500	15.000	22.500
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	SGD	Boete per maand: 25		
Zweden	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	SEK	175.000	245.000	315.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	SEK	35.000	70.000	105.000
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	SEK	Boete per maand: 135		
Verenigd Koninkrijk	Niveau 1	Kaartaccepterend bedrijf of Serviceprovider	GBP	12.500	18.000	23.000
	Niveau 2	Kaartaccepterend bedrijf of Serviceprovider	GBP	2.500	5.000	7.500
	Niveau 3 en Niveau 4	Kaartaccepterend bedrijf	GBP	Boete per maand: 15		

Paragraaf 5 Vertrouwelijkheid

American Express zal redelijke maatregelen nemen om uw rapporten over naleving, inclusief de Valideringsdocumentatie, in vertrouwen te bewaren (en ervoor te zorgen dat zijn agenten en onderaannemers, inclusief SecureTrust dat eveneens doen), en de Valideringsdocumentatie niet aan derden bekend maken (anders dan aan gelieerde ondernemingen, agenten, vertegenwoordigers, Serviceproviders en onderaannemers van American Express) voor een periode van drie jaar vanaf de datum van ontvangst. Uitgezonderd op deze geheimhoudingsverplichting is Valideringsdocumentatie die:

- a. al vóór de openbaarmaking bekend is bij American Express;
- b. beschikbaar is of voor het publiek wordt zonder inbreuk op deze paragraaf door American Express;
- c. rechtmatig door American Express van een derde is ontvangen zonder geheimhoudingsplicht;
- d. onafhankelijk is ontwikkeld door American Express; of
- e. openbaar moet worden gemaakt door een gerechtelijk bevel of overheidsinstantie, of door enige wet, regel of regelgeving, of door dagvaarding, verzoek tot openbaring, dagvaarding of ander administratief of juridisch proces, of door een formeel of informeel verzoek of onderzoek door een overheidsinstantie of autoriteit (inclusief een regelgevende instantie, inspecteur, onderzoeker of wetshandhavingsinstantie).

Paragraaf 6 Disclaimer

AMERICAN EXPRESS WIJST HIERBIJ ALLE VERKLARINGEN, GARANTIES EN AANSPRAKELIJKHEDEN AF MET BETREKKING TOT DEZE DATA SECURITY OPERATING POLICY DE PCI DSS, DE EMV-SPECIFICATIES EN DE AANWIJZING EN UITVOERING VAN QSA'S, ASV'S OF PFI'S (OF ÉÉN VAN DEZE), EXPLICIET, IMPLICIET, WETTELIJK OF ANDERSZINS, MET INBEGRIIP VAN ELKE GARANTIE VAN VERKOOPBAARHEID OF GESCHIKTHEID VOOR EEN BEPAALD DOEL. AMERICAN EXPRESS-KAARTUITGEVENDE BEDRIJVEN ZIJN GEEN DERDE BEGUNSTIGDEN ONDER DIT BELEID.

Nuttige websites

American Express-gegevensbeveiliging: www.americanexpress.com/datasecurity

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

Woordenlijst

Alleen voor de doeleinden van deze [Data Security Operating Policy \(DSOP\)](#) zijn de volgende definities van toepassing en hebben controle in het geval van een conflict met de termen in de *Regelgeving voor Kaartaccepterende bedrijven*.

American Express-kaart, of **kaart**, betekent elke kaart, apparatuur met toegang tot uw rekening, betaalapparaat of dienst met de naam, het logo, het handelsmerk, het servicemerk, de handelsnaam of een ander eigen ontwerp of aanduiding van American Express of een gelieerde onderneming en uitgegeven door een uitgever of een kaartrekeningnummer.

Attest van naleving (Attestation of Compliance, AOC) is een verklaring van de status van uw naleving van de PCI DSS, in het formulier dat verstrekt is door de Payment Card Industry Security Standards Council, LLC.

Attest van naleving van scanregels (Attestation of Scan Compliance, AOSC) is een verklaring van de status van uw naleving van de PCI DSS op basis van een netwerkscan, in het formulier dat verstrekt is door de Payment Card Industry Security Standards Council, LLC.

Betaaltoepassing heeft de betekenis die de term 'Payment Application' kreeg in de toen actuele verklarende woordenlijst van de Payment Card Industry Payment Application Data Security Standard; deze vindt u op www.pcisecuritystandards.org.

Betaling is een betaling of aankoop gedaan met een kaart.

Buyer Initiated Payment-transacties (BIP) zijn betalingstransacties die mogelijk zijn gemaakt via een betalingsinstructiebestand dat is verwerkt via BIP.

Chip is een geïntegreerde microchip die is ingesloten op een kaart met Kaarthouder- en rekeninginformatie.

Chipapparaat betekent een POS-apparaat met een geldige en actuele goedkeuring/certificering van EMVCo (www.emvco.com) dat in staat is om AEIPS-compatibele chipkaarttransacties te verwerken.

Chipkaart betekent een kaart met een Chip waarvoor mogelijk een pincode nodig is om de identiteit van de Kaarthouder of de rekeninginformatie op de Chip te verifiëren (in onze documentatie ook wel 'smartcard', 'EMV-kaart', 'ICC' of 'integrated circuit card' genoemd).

Coderingssleutel (coderingssleutel van American Express) is de sleutel die wordt gebruikt bij het verwerken, genereren, laden en/of beschermen van rekeninggegevens. Dit omvat, maar is niet beperkt tot het volgende:

- Sleutelcoderingssleutels (Key Encrypting Keys, Kek's): Zonehoofdsleutels (Zone Master Keys, ZMK's) en zonepincodesleutels (Zone Pin Keys, ZPK's)
- Hoofdsleutels (ZMK's) die worden gebruikt in beveiligde cryptografische apparaten: lokale hoofdsleutels (LMK's)
- Kaartbeveiligingscodesleutels (Card Security Code Keys, CSCK's)
- Pincodesleutels: basisderivatiesleutels (Base Derivation Keys, BDK's), pincoderingssleutels (PIN Encryption Key, PEK's) en ZPK's

Derde partijen zijn uw werknemers, agenten, vertegenwoordigers, onderaannemers, verwerkers, Serviceproviders, leveranciers van uw point-of-sale-apparatuur (POS), kassasystemen of betalingsverwerkers, of entiteiten die zijn gekoppeld aan uw American Express-Kaartaccepterende bedrijvenaccount, en iedere andere partij aan wie u toegang tot de Kaarthouderinformatie verleent in overeenstemming met de Overeenkomst.

EMV-specificaties zijn de door EMVCo LLC uitgegeven specificaties die te raadplegen zijn op www.emvco.com.

EMV-transactie betekent een transactie met een integrated circuit card (ook wel 'IC-kaart', 'chipkaart', 'smartcard', 'EMV-kaart' of 'ICC' genoemd) die wordt uitgevoerd bij een terminal van een Point of Sale (POS) die geschikt is voor chipkaarten en van een geldig en actueel goedgekeurd EMV-type is. EMV-goedkeuringen zijn beschikbaar op www.emvco.com.

Enquête voor zelfbeoordeling (Self-Assessment Questionnaire, SAQ) is een hulpmiddel voor zelfbeoordeling dat is ontwikkeld door de Payment Card Industry Security Standards Council, LLC, bedoeld om de naleving van de PCI DSS te evalueren en te bevestigen.

Franchisegever is de exploitant van een bedrijf dat personen of entiteiten (franchisenemers) de licentie geeft om goederen en/of diensten te distribueren onder, of te opereren met gebruikmaking van het handelsmerk van de exploitant. Deze assisteert franchisenemers bij het runnen van hun bedrijf of beïnvloedt de werkwijze van de franchisenemer, en vereist betaling van een vergoeding door franchisenemers.

Gecompromitteerd kaartnummer betekent dat een American Express Card-rekeningnummer verband houdt met een Gegevensincident.

Gegevensincident is een incident waarbij de Coderingssleutels van American Express zijn gecompromitteerd of vermoedelijk gecompromitteerd, of minimaal één American Express Card-rekeningnummer met:

- onbevoegde toegang tot of gebruik van Coderingssleutels, Kaarthouderinformatie of Gevoelige verificatiegegevens (of een combinatie hiervan) die worden opgeslagen, verwerkt of verzonden op uw apparatuur, systemen en/of netwerken (of de componenten daarvan) in uw eigendom of waarvan u een gebruikersmachtiging afgeeft;
- gebruik van dergelijke Coderingssleutels, Kaarthouderinformatie of Gevoelige verificatiegegevens (of een combinatie hiervan) anders dan in overeenstemming met de Overeenkomst; en/of
- vermoedelijk of bevestigd verlies, diefstal of verduistering op welke manier dan ook van media, materialen, gegevens of informatie die dergelijke Coderingssleutels, Kaarthouderinformatie of Gevoelige verificatiegegevens bevatten (of een combinatie hiervan).

Gegevensincidentperiode is de periode die begint op de datum van de betrokkenheid, indien bekend, of 365 dagen voorafgaand aan de Notificatiedatum als de feitelijke datum van de betrokkenheid onbekend is. De Gegevensincidentperiode eindigt 30 dagen na de Notificatiedatum.

Gevoelige verificatiegegevens heeft de betekenis die de term 'Sensitive Authentication Data' kreeg in de toen actuele verklarende woordenlijst van de PCI DSS.

Goedgekeurde oplossing voor point-to-point-codering (P2PE), opgenomen in de PCI SSC-lijst met gevalideerde oplossingen of gevalideerd door een door PCI SSC gekwalificeerd Security Assessor P2PE-bedrijf.

Goedgekeurde scanprovider (Approved Scan Vendor, ASV) is een entiteit die is gekwalificeerd door de Payment Card Industry Security Standards Council, LLC om de naleving van bepaalde PCI DSS-vereisten te valideren door middel van het uitvoeren van kwetsbaarheidsscans op omgevingen die met het internet zijn verbonden.

Kaartaccepterend bedrijf is het Kaartaccepterend bedrijf en al zijn gelieerde bedrijven die American Express-kaarten accepteren onder een Overeenkomst met American Express of zijn gelieerde bedrijven.

Kaartaccepterend bedrijf van niveau 1 is een Kaartaccepterend bedrijf met 2,5 miljoen American Express-kaarttransacties of meer per jaar, of elke Kaartaccepterend bedrijf die American Express anderszins als niveau 1 beschouwt.

Kaartaccepterend bedrijf van niveau 2 is een Kaartaccepterend bedrijf met 50.000 tot 2,5 miljoen American Express-kaarttransacties per jaar.

Kaartaccepterend bedrijf van niveau 3 is een Kaartaccepterend bedrijf met 10.000 tot 50.000 American Express-kaarttransacties per jaar.

Kaartaccepterend bedrijf van niveau 4 is een Kaartaccepterend bedrijf met minder dan 10.000 American Express-kaarttransacties per jaar.

Kaarthouder is de persoon of entiteit (i) die een overeenkomst is aangegaan om een kaartrekening te openen met een uitgever of (ii) wiens naam op de kaart staat.

Kaarthouderinformatie heeft de betekenis die de term 'Cardholder Data' kreeg in de toen actuele verklarende woordenlijst van de PCI DSS.

Kaarthouderinformatie is informatie over American Express-Kaarthouders en kaarttransacties, inclusief namen, adressen, kaartrekeningnummers en kaartidentificatienummers (CID's).

Krediet betekent het bedrag van de Betaling dat u terugstort aan Kaarthouders voor aankopen of betalingen die met de kaart zijn gedaan.

Notificatiedatum betekent een door American Express vastgestelde datum waarop uitgevers een melding ontvangen van het Gegevensincident. Een dergelijke datum is afhankelijk van de ontvangst door American Express van het definitieve forensische rapport of de interne analyse en wordt naar eigen goeddunken van American Express bepaald.

Payment Card Industry Security Standards Council (PCI SSC) -vereisten zijn de reeks standaarden en vereisten met betrekking tot het beveiligen en beschermen van betaalkaartgegevens, inclusief PCI DSS en PA DSS, beschikbaar op www.pcisecuritystandards.org.

PCI DSS staat voor Payment Card Industry Data Security Standards die beschikbaar zijn op www.pcisecuritystandards.org.

PCI Forensic Investigator (PFI) is een entiteit die is goedgekeurd door de Payment Card Industry Security Standards Council, LLC om forensisch onderzoek uit te voeren naar een inbreuk op of compromittering van betaalkaartgegevens.

PCI-goedgekeurd betekent dat een Pinapparaat of betaaltoepassing (of beide) op het tijdstip van inzet verschijnt op de lijst van goedgekeurde bedrijven en leveranciers die wordt bijgehouden door de PCI Security Standards Council, LLC; deze vindt u op www.pcisecuritystandards.org.

PCI PIN Security Requirements betekent de vereisten van de Payment Card Industry voor pincodebeveiliging; deze zijn beschikbaar op www.pcisecuritystandards.org.

Pinapparaat heeft de betekenis die de term 'PIN Entry Device' kreeg in de toen actuele verklarende woordenlijst van de Payment Card Industry PIN Transaction Security (PTS), Point of Interaction (POI), Modular Security Requirements, die beschikbaar zijn op www.pcisecuritystandards.org.

Point of Sale (POS) -systeem betekent een systeem of apparaat voor informatieverwerking, waaronder een terminal, pc, elektronische kassa, contactvrije scanner of betaalautomaat of -proces, gebruikt door een Kaartaccepterend bedrijf om autorisatie te verkrijgen en/of transactiegegevens te verzamelen.

Point-to-Point-codering (P2PE) is een oplossing die rekeninggegevens cryptografisch beschermt vanaf het punt waarop een Kaartaccepterend bedrijf de betaalkaart accepteert tot aan het beveiligde punt van decodering.

Preventieve technologie betekent technologische oplossingen die de beveiliging van American Express-Kaarthouderinformatie en Gevoelige verificatiegegevens verbeteren, zoals bepaald door American Express. Om te worden beschouwd als een Preventieve technologie, moet u aantonen dat de technologie effectief wordt gebruikt in overeenstemming met het ontwerp en het beoogde doel. Voorbeelden zijn onder andere: EMV, Point-to-Point-codering en het gebruik van tokens.

Processor is een Serviceprovider voor Kaartaccepterende bedrijven die verwerking van autorisatie en indiening bij het American Express-netwerk mogelijk maakt.

Programma voor verbeteringen van beveiligingstechnologie (Security Technology Enhancement Program, STEP) is het American Express-programma waarin Kaartaccepterende bedrijven worden aangemoedigd om technologieën in te zetten die de gegevensbeveiliging verbeteren. Om in aanmerking te komen voor STEP, mogen Kaartaccepterende bedrijven in de 12 maanden voorafgaand aan het indienen van het jaarlijkse STEP-attest geen Gegevensincident hebben gehad en moeten zij minstens 75% van alle transacties uitvoeren met Point-to-Point-codering of persoonlijke transacties op een EMV-apparaat met een chipfunctie.

Qualified Security Assessor (QSA) betekent een entiteit die is gekwalificeerd door de Payment Card Industry Security Standards Council, LLC om naleving van de PCI DSS te valideren.

Samenvatting van naleving (Summary of Compliance, SOC) is een PCI-valideringsdocument dat door een franchisegever of Serviceprovider wordt gebruikt om de PCI-nalevingsstatus van de betrokken franchisenemers aan te geven.

Serviceprovider betekent een geautoriseerde processor, externe processor, gatewayleverancier, integratoren van POS-systemen of een andere entiteit die aan Kaartaccepterende bedrijven van POS-systemen of andere oplossingen of services voor de verwerking van betalingen levert.

Serviceprovider van niveau 1 is een Serviceprovider met 2,5 miljoen American Express-kaarttransacties of meer per jaar, of een Serviceprovider die American Express anderszins als een niveau 1 beschouwt.

Serviceprovider van niveau 2 is een Serviceprovider met minder dan 2,5 miljoen American Express-kaarttransacties per jaar, of een Serviceprovider die door American Express niet als niveau 1 wordt beschouwd.

Transactie betekent een betaling of krediet die of dat wordt voltooid met een kaart.

Valideringsdocumentatie staat voor het AOC dat is opgesteld in verband met een jaarlijkse veiligheidsbeoordeling of SAQ ter plaatse, de AOSC en executive summary's van bevindingen die zijn opgesteld in verband met driemaandelijke netwerkscans, of het jaarlijkse attest van het programma voor verbeteringen van beveiligingstechnologie.