AMERICAN EXPRESS

Data Security Operating Policy (DSOP)

Wijzigingsbalken

Belangrijke updates staan vermeld in de tabel Samenvatting van Wijzigingen en worden ook in de DSOP met een aangegeven. Wijzigingsbalken zijn verticale lijnen in de linkermarge die herziene, toegevoegde of verwijderde tekst identificeren. Alle wijzigingen in de DSOP worden aangegeven met een wijzigingsbalk, zoals hier weergegeven.

Tabel Samenvatting van Wijzigingen

Belangrijke updates staan vermeld in de onderstaande tabel en worden ook in de *DSOP* met een wijzigingsbalk aangegeven.

Paragraaf/subparagraaf	Beschrijving van wijziging
Er zijn geen wijzigingen voor deze versie.	

Wat te doen bij een Gegevensincident?

Volg a.u.b deze stappen wanneer u in uw bedrijf een Gegevensincident heeft geïdentificeerd.

Stap 1:

Vul het Formulier Eerste Melding Bedrijfsgegevensincident in en e-mail het naar EIRP@aexp.com, niet later dan 72 uur nadat het Gegevensincident is ontdekt.

Stap 2:

Voer een gedegen onderzoek uit; hiervoor moet u mogelijk een Payment Card Industry (PCI) Forensic Investigator inhuren.

Stap 3:

Stuur ons onmiddellijk alle gecompromitteerde American Express® Kaartnummers.

Stap 4:

Werk met ons samen om eventuele problemen die voortvloeien uit het Gegevensincident op te lossen.

Zie Paragraaf 3, "Verplichtingen omtrent Beheer van Gegevensincidenten" voor meer informatie over Verplichtingen omtrent Beheer van Gegevensincidenten.

Heeft u meer vragen?

VS: (888) 732-3750 (gratis)

Internationaal: +1 (602) 537-3021

EIRP@aexp.com

Als toonaangevende onderneming op het gebied van consumentenbescherming legt American Express zich er reeds lang op toe Kaarthoudergegevens 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 Kaartuitgevers. 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 bedrijf verbeteren.

American Express weet dat onze Kaartaccepterende Bedrijven en Serviceproviders (gezamenlijk u) onze zorg delen en vereist, als onderdeel van uw verantwoordelijkheden, dat **u** voldoet aan de bepalingen inzake gegevensbeveiliging in uw **Overeenkomst** om deze te accepteren (in het geval van Kaartaccepterende Bedrijven) of te verwerken (in het geval van Serviceproviders) de American Express® Kaart (elk respectievelijk de Overeenkomst) en deze Data Security Operating Policy (operationele policy voor gegevensbeveiliging), 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, Kaarthoudergegevens 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 deze policy.

Paragraaf 1 Targeted Analysis Programme (TAP)

Compromitteringen van Kaarthoudergegevens kunnen worden veroorzaakt door hiaten in de gegevensbeveiliging in uw Omgeving van Kaarthoudergegevens (CDE).

Voorbeelden van een Compromittering van Kaarthoudergegevens zijn, maar zijn niet beperkt tot:

- **Gemeenschappelijk verkooppunt (CPP):** American Express Kaarthouders melden frauduleuze Transacties op hun Kaartrekeningen en worden geïdentificeerd en er wordt vastgesteld dat ze afkomstig zijn van aankopen bij uw Kaartaccepterende Bedrijven.
- **Kaarthoudergegevens gevonden:** American Express Kaart- en Kaarthoudergegevens gevonden op internet en gelinkt naar Transacties bij uw Kaartaccepterende Bedrijven.
- **Verdenking van malware:** American Express vermoedt dat u software gebruikt die is geïnfecteerd met of kwetsbaar is voor schadelijke code.

TAP is ontworpen om mogelijke compromittering van Kaarthoudergegevens te identificeren.

U moet voldoen aan de volgende vereisten na kennisgeving door American Express van een mogelijke compromittering van Kaarthoudergegevens, en u moet zorgen dat uw Gebonden Partijen hieraan voldoen.

- U moet onmiddellijk uw CDE controleren op lacunes in de gegevensbeveiliging en eventuele bevindingen verhelpen.
  - U moet uw externe leverancier(s) ertoe brengen een grondig onderzoek naar uw CDE uit te voeren als dit wordt uitbesteed.
- U moet na kennisgeving door American Express een samenvatting van de ondernomen of geplande maatregelen na uw beoordeling, evaluatie en/of herstelinspanningen verstrekken.
- U moet bijgewerkte PCI DSS-valideringsdocumenten verstrekken in overeenstemming met Paragraaf 5, "Belangrijke periodieke validatie van uw systemen",
- Indien van toepassing, moet u een gekwalificeerde PCI Forensic Investigator (PFI) inschakelen om uw CDE te onderzoeken als u of uw Gebonden Partij:
  - De compromittering van de Kaarthoudergegevens niet binnen een redelijke termijn kunt oplossen, zoals bepaald door American Express, of
  - Bevestigt dat zich een Gegevensincident heeft voorgedaan en voldaan is aan de vereisten uiteengezet in Paragraaf 3, "Verplichtingen omtrent Beheer van Gegevensincidenten".

Tabel A-1: TAP-kosten voor niet-naleving

Beschrijving	Kaartaccepterend Bedrijf van niveau 1 of Serviceprovider van niveau 1	Kaartaccepterend Bedrijf van niveau 2 of Serviceprovider van niveau 2	Kaartaccepterend Bedrijf van niveau 3 of niveau 4
Een boete voor niet valideren kan worden opgelegd als niet aan de TAP-verplichtingen is voldaan voor de eerste deadline.	USD $25.000	USD $5.000	USD $1.000
Een boete voor niet valideren kan worden opgelegd als niet aan de TAP-verplichtingen is voldaan voor de tweede deadline.	USD $35.000	USD $10.000	USD $2.500
Een boete voor niet valideren kan worden opgelegd als niet aan de TAP-verplichtingen is voldaan voor de derde deadline. **OPMERKING:** *Boetes voor niet-naleving kunnen worden toegepast totdat aan de verplichtingen is voldaan of totdat TAP is opgelost.*	USD $45.000	USD $15.000	USD $5.000

Als niet aan uw TAP-verplichtingen wordt voldaan, heeft American Express het recht om de niet-nalevingskosten cumulatief op te leggen, betalingen in te houden en/of de Overeenkomst te beëindigen.

Paragraaf 2 Standaarden voor de bescherming van Coderingssleutels, Kaarthoudergegevens en Gevoelige Verificatiegegevens

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

- Kaarthoudergegevens 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 Kaarthoudergegevens of Gevoelige Verificatiegegevens niet later dan de ingangsdatum van de implementatie van die versie van het toepasselijke vereiste.
- alleen door de PCI goedgekeurde nieuwe of vervangende Pinapparaten of Betaaltoepassingen (of beide) gebruiken.

U dient alle American Express-Charge- en Crediteringsoverzichten te beschermen waarover u in overeenstemming met deze bepalingen betreffende beveiliging van gegevens beschikt. U mag deze overzichten alleen gebruiken voor doeleinden vermeld in deze Overeenkomst en moet deze op gepaste wijze beveiligen.
U bent financieel en anderszins aansprakelijk jegens American Express om ervoor te zorgen dat de Gebonden Partijen waar u mee werkt, deze bepalingen betreffende gegevensbeveiliging naleven (anders dan om aan te tonen dat uw Gebonden Partijen deze policy naleven onder Paragraaf 5, "Belangrijke periodieke validatie van uw systemen", tenzij anders voorzien in die paragraaf).

Paragraaf 3 Verplichtingen omtrent Beheer van Gegevensincidenten

U moet American Express onmiddellijk en in geen geval later dan tweeëntwintig (72) uur na ontdekking van een Gegevensincident op de hoogte stellen.

Neem contact op met het American Express Enterprise Incident Response-programma (*EIRP*) om American Express op de hoogte te stellen op +1 (602) 537-3021 (+ geeft het internationale landnummer (International Direct Dial, 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. Daarnaast:

- 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.
- U moet 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.

Naast de voorgaande paragrafen in deze Paragraaf 3, "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 voor Gegevensincidenten waarbij minder dan 10.000 unieke Kaartnummers zijn betrokken. Een dergelijk onderzoek moet voldoen aan de vereisten die hierboven in deze Paragraaf 3, "Verplichtingen omtrent Beheer van Gegevensincidenten" zijn uiteengezet en moet binnen de door American Express vereiste periode worden voltooid.
- American Express kan 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 de Overeenkomst.

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

Paragraaf 4 Schadeloosstellingsverplichtingen bij 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 Paragraaf 4, "Schadeloosstellingsverplichtingen bij een Gegevensincident". Naast uw schadeloosstellingsverplichtingen (indien van toepassing), kunt u onderworpen zijn aan een vergoeding voor niet-naleving van Gegevensincidenten, zoals hieronder beschreven in Paragraaf 4, "Schadeloosstellingsverplichtingen bij 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 hebt American Express geinformeerd over het Gegevensincident conform Paragraaf 3, "Verplichtingen omtrent Beheer van Gegevensincidenten",
  - 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 Gebonden Partijen.

Ondanks de voorgaande paragrafen in Paragraaf 4, "Schadeloosstellingsverplichtingen bij een Gegevensincident", betaalt u voor elk Gegevensincident, ongeacht het aantal American Express Kaartnummers, aan American Express een vergoeding voor niet-naleving van de voorschriften voor Gegevensincidenten van niet meer dan $ 100.000 USD per Gegevensincident (zoals naar eigen goeddunken bepaald door American Express) in het geval dat u één van uw verplichtingen niet nakomt, zoals uiteengezet in Paragraaf 3, "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 elk American Express Card-rekeningnummer van de berekening uitsluiten dat betrokken was bij een eerdere claim tot schadeloosstelling van een Gegevensincident die werd ingediend binnen twaalf (12) maanden voorafgaand aan de Kennisgevingsdatum. 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 schadeloosstellingsverplichtingen voor Gegevensincidenten in rekening brengen of het bedrag aftrekken van betalingen van American Express aan u (of uw Bankrekening dienovereenkomstig debiteren).

Uw schadeloosstellingsverplichtingen in geval van Gegevensincidenten zullen niet worden beschouwd als incidentele, indirecte, speculatieve, gevolg-, speciale, punitieve of voorbeeldschade onder deze Overeenkomst, op voorwaarde dat dergelijke verplichtingen geen schade omvatten 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 schadeloosstellingsverplichtingen 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 Kaarthoudergegevens 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:

Tabel A-2: Vereiste criteria Verlaging van de schadeloosstellingsverplichting

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 op >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 Chipcards 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.

Tabel A-3: Extra verlaging van de schadeloosstellingsverplichting

Bijv.	Preventieve technologieën in gebruik	Komt in aanmerking	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 alle Transacties op Apparaten met een Chipfunctie	Ja	77%: Extra verlaging (gebaseerd op 77% gebruik van Preventieve technologie)
	77% van de locaties gebruikt andere Preventieve technologie		

Bijv.	Preventieve technologieën in gebruik	Komt in aanmerking	Verlaging
3	93% van alle Transacties op Apparaten met een Chipfunctie 100% van de locaties gebruikt andere Preventieve technologie	Ja	93%: Extra verlaging (gebaseerd op 93% van de Transacties op Apparaten met een Chipfunctie)
4	40% van alle Transacties op Apparaten met een Chipfunctie 90% van de locaties gebruikt andere Preventieve technologie	Nee	50%: Standaardverlaging (minder dan 75% van Transacties op Apparaten met een Chipfunctie kwalificeert niet voor een extra verlaging)

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

Paragraaf 5 Belangrijke periodieke validatie van uw systemen

U moet, zoals hieronder beschreven, jaarlijks en om de 90 dagen de volgende acties met betrekking tot PCI DSS ondernemen om de status te valideren van de apparatuur, systemen en/of netwerken (en hun componenten) van u en uw Franchisenemers waarop Kaarthoudergegevens of Gevoelige Verificatiegegevens worden opgeslagen, verwerkt of verzonden.

Er zijn vier acties vereist om aan validatie te voldoen:

Actie 1: Deelnemen aan het PCI nalevingsprogamma ("het Programma") van American Express conform deze policy.

Actie 2: Uw Niveau van Kaartaccepterend Bedrijf en Valideringsvereisten begrijpen.

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

Actie 4: De Valideringsdocumentatie versturen naar American Express binnen de voorgeschreven deadlines.

Actie 1: Deelnemen aan het Nalevingsprogramma van American Express conform deze Policy

Kaartaccepterende Bedrijven van niveau 1, Kaartaccepterende Bedrijven van niveau 2 en alle Serviceproviders zoals hieronder beschreven, moeten deelnemen aan het Programma conform deze policy. American Express kan naar eigen goeddunken specifieke Kaartaccepterende Bedrijven van niveau 3 en niveau 4 aanwijzen om deel te nemen aan het Programma conform deze policy.

Kaartaccepterende Bedrijven en Serviceproviders die verplicht zijn aan het Programma deel te nemen, moeten zich binnen de voorziene tijd inschrijven op de Portal verstrekt door de Programmabeheerder die door American Express is geselecteerd.

- U moet alle redelijke voorwaarden aanvaarden die met het gebruik van de Portal verband houden.
- U moet ten minste één contactpersoon gegevensbeveiliging aanwijzen en de juiste informatie over die persoon verstrekken aan de Portal. Vereiste gegevenselementen omvatten:
  - volledige naam
  - e-mailadres
  - telefoonnummer
  - fysiek postadres
- U moet bijgewerkte of nieuwe contactinformatie voor de aangewezen contactpersoon gegevensbeveiliging aan de Portal verstrekken wanneer de informatie wijzigt.

- U moet erop toezien dat uw systemen zijn bijgewerkt om servicecommunicatie van het aangewezen Portaldomein mogelijk te maken.

Als u nalaat actuele gegevens over de contactpersoon gegevensbeveiliging te verstrekken of bij te houden, of nalaat e-mailcommunicatie mogelijk te maken, zal dit geen invloed hebben op onze rechten om boetes aan te rekenen.

Actie 2: Uw Niveau van Kaartaccepterend Bedrijf en Valideringsvereisten begrijpen

Er zijn vier Niveaus van Kaartaccepterende Bedrijven van toepassing op Kaartaccepterende Bedrijven en twee niveaus van toepassing op Serviceproviders op basis van uw aantal American Express Kaarttransacties.

- Voor Kaartaccepterende Bedrijven is dit het door hun bedrijven ingediende volume dat doorloopt naar het hoogste American Express rekeningniveau voor Kaartaccepterende Bedrijven.*
- Voor Serviceproviders is dit de som van het volume ingediend door de Serviceprovider en de Entitiesserviceprovider aan wie u services verstrekt.

Buyer Initiated Payments-transacties (BIP) zijn niet inbegrepen in het volume van American Express Kaarttransacties om het niveau van het Kaartaccepterende Bedrijf en de valideringsvereisten te bepalen. U valt in één van de niveaus die zijn gespecificeerd in de onderstaande tabellen voor Kaartaccepterende Bedrijven en Serviceproviders.

* In het geval van Franchisegevers omvat dit het volume van de bedrijven 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.

Vereisten Valideringsdocumentatie van Kaartaccepterende Bedrijven

Kaartaccepterende Bedrijven (geen Serviceproviders) hebben vier mogelijke classificaties met betrekking tot hun niveau. Nadat u het niveau van het Kaartaccepterende Bedrijf uit de onderstaande lijst hebt bepaald, raadpleegt u de Tabel A-4: Valideringsdocumentatie Kaartaccepterend bedrijf 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 A-4: Valideringsdocumentatie Kaartaccepterend bedrijf

Niveau van Kaartaccepterend Bedrijf/Jaarlijkse American Express-transacties	Rapport Nalevingsverklaring van naleving (ROC AOC)	Enquête Nalevingsverklaring (SAQ AOC) EN Driemaandelijkse Scan van Kwetsbaarheden van Externe Netwerken (Scan)	STEP-verklaring voor in aanmerking komende Kaartaccepterende Bedrijven
Niveau 1/ 2,5 miljoen of meer	Verplicht	Niet van toepassing	Optioneel met goedkeuring van American Express (vervangt ROC)
Niveau 2/ 50.000 tot 2,5 miljoen	Optioneel	SAQ AOC verplicht (tenzij een ROC AOC wordt ingediend); scan verplicht met bepaalde SAQ-typen	Optioneel (vervangt SAQ en netwerkscan of ROC)

Niveau van Kaartaccepterend Bedrijf/Jaarlijkse American Express-transacties	Rapport Nalevingsverklaring van naleving (ROC AOC)	Enquête Nalevingsverklaring (SAQ AOC) EN Driemaandelijkse Scan van Kwetsbaarheden van Externe Netwerken (Scan)	STEP-verklaring voor in aanmerking komende Kaartaccepterende Bedrijven
Niveau 3/ 10.000 tot 50.000	Optioneel	SAQ AOC 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 AOC 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 volledigheid, juistheid en geschiktheid van uw PCI-valideringsdocumentatie te controleren. American Express kan eisen dat u, ter ondersteuning van dit doel, aanvullende ondersteunende documenten verstrekt ter beoordeling. Verder heeft American Express het recht om te eisen dat u een door de PCI Security Standards Council goedgekeurde QSA of PFI inschakelt.

Programma voor verbeteringen van beveiligingstechnologie (STEP)

Kaartaccepterende Bedrijven die aan PCI DSS voldoen, kunnen naar goeddunken van American Express 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 een combinatie van de volgende extra beveiligingsopties:

- **EMV, EMV Contactloze of Digitale Portemonnee** – 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 moeten ook Contactloos 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
- **Getokeniseerd** – de geïmplementeerde tokenisatieoplossing moet:
  - voldoen aan de EMVCo-specificaties,
  - beveiligd, verwerkt, opgeslagen, verzonden en volledig door een externe serviceprovider conform PCI worden beheerd, en
  - het Token kan niet worden teruggedraaid om niet-gemaskeerde Primaire rekeningnummers (PAN's) aan het Kaartaccepterende Bedrijf te onthullen.

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 versturen naar American Express" hieronder.

Vereisten voor Serviceproviders

Serviceproviders (geen Kaartaccepterende Bedrijven) hebben twee mogelijke classificaties met betrekking tot hun niveau. Nadat u het niveau van de Serviceprovider uit de onderstaande lijst hebt bepaald, raadpleegt u de Tabel A-5: Documentatie Serviceprovider 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 A-5: Documentatie Serviceprovider

Niveau	Valideringsdocumentatie	Vereiste
1	Jaarlijks Nalevingsrapport Nalevingsverklaring (ROC AOC)	Verplicht
2	Jaarlijkse SAQ D (Serviceprovider) en Driemaandelijkse Netwerkscan of Jaarlijks Nalevingsrapport Nalevingsverklaring (ROC AOC), indien dit de voorkeur heeft	Verplicht

Het wordt aanbevolen dat Serviceproviders ook voldoen aan de Aanvullende PCI-validatie voor aangewezen entiteiten.

Actie 3: De Valideringsdocumentatie invullen die u dient te versturen 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.

U moet de Verklaring van naleving (Attestation of Compliance, AOC) voor het toepasselijke type beoordeling indienen. De AOC is een verklaring van de status van uw naleving en moet daarom ondertekend en gedateerd worden door iemand van het geschikte leiderschapsniveau binnen uw organisatie.

Naast de AOC kan American Express eisen dat u een kopie verstrekt van de volledige beoordeling en, naar ons goeddunken, aanvullende ondersteunende documenten die naleving van de PCI DSS-vereisten aantonen. Het invullen van deze Valideringsdocumentatie gebeurt op uw kosten.

Nalevingsrapport Nalevingsverklaring (Report on Compliance Attestation of Compliance, ROC AOC) - (jaarlijks vereist) – Het Nalevingsrapport documenteert de resultaten van een gedetailleerd onderzoek ter plaatse van uw apparatuur, systemen en netwerken (en hun componenten) waar Kaarthoudergegevens of Gevoelige Verificatiegegevens (of beide) worden opgeslagen, verwerkt of verzonden. Er zijn twee versies: een voor Kaartaccepterende Bedrijven en een andere voor Serviceproviders. Het Nalevingsrapport moet worden opgesteld door:

- een QSA of
- door u en bevestigd door uw chief executive officer, chief financial officer, chief information security officer of principal officer

De AOC moet worden ondertekend en gedateerd door een QSA of een interne Security Assessor (ISA) en iemand van het bevoegde leiderschapsniveau binnen uw organisatie en ten minste eenmaal per jaar aan American Express worden verstrekt.

Nalevingsverklaring Enquête voor zelfbeoordeling (Self-Assessment Questionnaire Attestation of Compliance, SAQ AOC) - (jaarlijks vereist) – De Enquêtes voor zelfbeoordeling stellen u in staat zelf uw apparatuur, systemen en netwerken (en hun componenten) waar Kaarthoudergegevens of Gevoelige Verificatiegegevens (of beide) worden opgeslagen, verwerkt of verzonden, te onderzoeken. Er zijn meerdere versies van de SAQ. U kiest een of meerdere versies op basis van uw Omgeving van Kaarthoudergegevens.

De SAQ kan worden ingevuld door personeel van uw bedrijf dat bevoegd is om de vragen nauwkeurig en grondig te beantwoorden, of u kunt een QSA inschakelen. De AOC moet ondertekend en gedateerd worden door iemand van het bevoegde leiderschapsniveau binnen uw organisatie en ten minste eenmaal per jaar aan American Express worden verstrekt.

Scanoverzicht van kwetsbaarheden van externe netwerken door Goedgekeurde scanprovider (Approved Scanning Vendor External Network Vulnerability Scan Summary, ASV Scan) - (om de 90 dagen vereist) – Een scan van externe kwetsbaarheden is een test op afstand om mogelijke zwakke punten, kwetsbaarheden en verkeerde configuraties van met het internet verbonden componenten van uw Omgeving van Kaarthoudergegevens te helpen identificeren (bijv. websites, apps, webservers, mailservers, publieksgerichte domeinen, of hosts).

De ASV-scan moet worden uitgevoerd door een Goedgekeurde scanprovider (Approved Scanning Vendor, ASV).

Indien vereist door de SAQ moet het volgende ten minste om de 90 dagen bij American Express worden ingediend: het AVS-rapport over de Verklaring van naleving van Scanregels (Attestation of Scan Compliance, AOSC) of het executive overzicht met een telling van gescande doelen, certificering dat de resultaten voldoen aan PCI DSS-scanprocedures, en de nalevingsstatus ingevuld door ASV.

ROC AOC of STEP zijn niet vereist een AOSC of executive overzicht van de ASV Scan in te dienen tenzij er speciaal om wordt gevraagd. Voor alle duidelijkheid: scans zijn verplicht indien vereist door de toepasselijke SAQ.

Voor alle duidelijkheid: ASV zijn verplicht indien vereist door de toepasselijke SAQ.

Valideringsdocumentatie voor STEP-verklaring (STEP) - (jaarlijks vereist) – STEP is alleen beschikbaar voor Kaartaccepterende Bedrijven die voldoen aan de criteria in Actie 2: "Uw Niveau van Kaartaccepterend Bedrijf en Valideringsvereisten begrijpen" hierboven. Als uw bedrijf in aanmerking komt, moet u het STEP-verklaringsformulier jaarlijks invullen en bij American Express indienen. Het Jaarlijkse STEP-verklaringsformulier kan worden gedownload via de Portal.

Niet-naleving van PCI DSS - (jaarlijks, om de 90 dagen en/of ad hoc vereist) – Als u niet voldoet aan de PCI DSS, moet u een van de volgende documenten overleggen:

- een Verklaring van naleving (AOC), inclusief "Deel 4. Actieplan in geval van niet-naleving" (kan worden gedownload via de PCI Security Standards Council-website)
- een Geprioriteerde aanpaksamenvatting van de PCI (kan worden gedownload via de PCI Security Standards Council-website)
- een Projectplansjabloon (kan worden gedownload via de Portal). Een Projectplan kan worden ingediend in plaats van de jaarlijkse verklaring (SAQ/ROC) en/of in plaats van de scan.

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 twaalf (12) maanden van de datum van het document te liggen. 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). Herstelacties die nodig zijn om naleving van PCI DSS tot stand te brengen, zijn op uw kosten.

Herstelacties die nodig zijn om naleving van PCI DSS tot stand te brengen, zijn op uw kosten.

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 u bent onderworpen aan alle andere bepalingen van deze policy.

Voor alle duidelijkheid, Kaartaccepterende Bedrijven die niet voldoen aan PCI DSS komen niet in aanmerking voor STEP.

Actie 4: De Valideringsdocumentatie versturen naar American Express

Alle Kaartaccepterende Bedrijven en Serviceproviders die verplicht deelnemen aan het Programma moeten de Valideringsdocumentatie indienen die als ‘verplicht’ is gemarkeerd in de tabellen in Actie 2: "Uw Niveau van Kaartaccepterend Bedrijf en Valideringsvereisten begrijpen" bij American Express binnen de toepasselijke deadlines.

U moet uw Valideringsdocumentatie bij American Express indienen via de Portal verstrekt door de Programmabeheerder die door American Express is geselecteerd. Door uw Valideringsdocumentatie in te dienen, verklaart en garandeert u American Express dat het volgende waar is (naar uw beste weten):

- Uw beoordeling was volledig en grondig;
- De PCI DSS-status is nauwkeurig weergegeven ten tijde van het invullen, ongeacht of het om naleving of niet-naleving gaat;
- U bent gemachtigd om de informatie daarin vrij te geven en de Valideringsdocumentatie aan American Express te verstrekken zonder de rechten van een andere partij te schenden.

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 driemaandelijkse rapportageperiode afzonderlijk informeren over de toepasselijke deadline.

Tabel A-6: Boete voor niet valideren

Beschrijving*	Kaartaccepterend Bedrijf van niveau 1 of Serviceprovider van niveau 1	Kaartaccepterend Bedrijf van niveau 2 of Serviceprovider van niveau 2	Kaartaccepterend Bedrijf van niveau 3 of van niveau 4
Indien de Valideringsdocumentatie niet voor de eerste deadline is ontvangen, wordt een boete voor niet valideren in rekening gebracht.	USD $25.000	USD $5.000	USD $50
Indien de Valideringsdocumentatie niet voor de tweede deadline is ontvangen, wordt een extra boete voor niet valideren in rekening gebracht.	USD $35.000	USD $10.000	USD $100
Indien de Valideringsdocumentatie niet voor de derde deadline is ontvangen, wordt een extra boete voor niet valideren in rekening gebracht. **OPMERKING:** Boetes voor niet valideren worden opgelegd tot de Valideringsdocumentatie wordt ingediend.	USD $45.000	USD $15.000	USD $250

* Boetes voor niet valideren worden berekend in equivalenten in de Lokale Munteenheid.

* Niet van toepassing in Argentinië.

Als niet aan uw verplichtingen betreffende PCI DSS-valideringsdocumentatie is voldaan, heeft American Express het recht om niet-valideringsboetes cumulatief op te leggen, betalingen in te houden en/of de Overeenkomst te beëindigen.

Paragraaf 6 Vertrouwelijkheid

American Express zal redelijke maatregelen nemen om uw rapporten over naleving, inclusief de Valideringsdocumentatie, vertrouwelijk te bewaren (en ervoor zorgen dat zijn agenten en onderaannemers, inclusief de Portalbeheerder 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 wordt voor het publiek 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, door enige wet, regel of regelgeving, 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 7 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 INBEGRIP 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 gelden deze in het geval van een conflict met de voorwaarden in het *Reglement 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.

Betaaltoepassing heeft de betekenis die eraan wordt gegeven in de op dat moment geldende Verklarende Woordenlijst voor Secure Software Standard en Secure Software Life Cycle Standard; deze vindt u op www.pcisecuritystandards.org.

Buyer Initiated Payments-transacties (BIP) zijn door de koper geïnitieerde Transacties die mogelijk zijn gemaakt via een betalingsinstructiebestand via BIP.

Charge is een betaling of aankoop die met een Kaart wordt gedaan.

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 rekening gegevens. 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 die worden gebruikt in beveiligde cryptografische apparaten: Lokale hoofdsleutels (Local Master Keys, 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

Creditering is het bedrag van de Charge dat u terugstort aan Kaarthouders voor aankopen of betalingen die met de Kaart zijn gedaan.

Eindrapportsjabloon Forensisch Incident betekent de sjabloon die verkrijgbaar is bij de PCI Security Standards Council, via www.pcisecuritystandards.org.

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

EMV-transactie betekent een Transactie met een integrated circuit card (ook wel 'IC-kaart', 'chipcard', 'smartcard', 'EMV-kaart' of 'ICC' genoemd) die wordt uitgevoerd bij een terminal van een Point of Sale (POS) die geschikt is voor IC-kaarten 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.

Franchisenemer is een onafhankelijke beheerde derde partij (inclusief een franchisenemer, licentiehouder of chapter), anders dan een Gelieerde Onderneming, die een vergunning heeft verkregen van een Franchisegever om een franchise te exploiteren en een schriftelijke overeenkomst is aangegaan met de Franchisegever waarbij deze consequent en prominent een externe identificatie weergeeft van de Merken van de Franchisegever of zich aan het publiek presenteert als lid van de bedrijvengroep van de Franchisegever.

Gebonden Partijen zijn uw werknemers, agenten, vertegenwoordigers, onderaannemers, Processors, Serviceproviders, leveranciers van uw point-of-sale-apparatuur (POS), kassasystemen of betalingsverwerkers, Entiteiten die zijn gekoppeld aan uw Kaartaccepterend Bedrijfsaccount van American Express, en iedere andere partij aan wie u toegang tot Kaarthouderinformatie verleent in overeenstemming met de Overeenkomst.

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 of beschikbaar maakt;
- 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 betekent de periode van inbraak (of een soortgelijke bepaalde tijdsperiode) zoals uiteengezet in het definitieve forensische rapport (bijv. PFI-rapport) of, indien onbekend, tot 365 dagen vóór de laatste Kennisgevingsdatum van mogelijk Gecompromitteerde Kaartnummers die betrokken zijn bij een Compromittering van Gegevens dat aan ons is gerapporteerd.

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 Scanning 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.

Gevoelige Verificatiegegevens heeft de betekenis die eraan wordt gegeven in de op dat moment geldende Verklarende Woordenlijst van de PCI DSS (*'Sensitive Authentication Data'*).

Kaartaccepterend Bedrijf is het Kaartaccepterend Bedrijf en al zijn Gelieerde Ondernemingen die American Express Kaarten accepteren onder een Overeenkomst met American Express of zijn Gelieerde Ondernemingen.

Kaartaccepterend Bedrijf van niveau 1 is een Kaartaccepterend Bedrijf met 2,5 miljoen American Express Kaarttransacties of meer per jaar, of een 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.

Kaarthoudergegevens heeft de betekenis die eraan wordt gegeven in de op dat moment geldende Verklarende Woordenlijst voor de PCI DSS (*'Cardholder Data'*).

Kaarthouderinformatie is informatie over American Express Kaarthouders en Kaarttransacties, inclusief namen, adressen, Kaartrekeningnummers en Kaartidentificatienummers (CID's).

Kaartnummer betekent het unieke identificatienummer dat de Uitgever aan de Kaart toekent wanneer deze wordt uitgegeven.

Kennisgevingsdatum betekent een door American Express vastgestelde datum waarop uitgevers een definitieve 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.

Niveau Kaartaccepterend Bedrijf betekent het niveau dat wij aan Kaartaccepterende Bedrijven toewijzen in verband met hun verplichtingen voor PCI DSS-nalevingsvalidering, zoals beschreven in Paragraaf 5, "Belangrijke periodieke validatie van uw systemen".

Omgeving van Kaarthoudergegevens (CDE) betekent de mensen, processen en technologie die kaarthoudergegevens of gevoelige authenticatiegegevens opslaan, verwerken of verzenden.

Payment Card Industry Data Security Standard (PCI DSS) staat voor de Payment Card Industry Data Security Standard die beschikbaar is op www.pcisecuritystandards.org.

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

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 Security Standards Council, LLC; deze vindt u op www.pcisecuritystandards.org.

Pinapparaat heeft de betekenis (*'PIN Entry Device'*) die eraan wordt gegeven in de op dat moment geldende Verklarende Woordenlijst voor 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, contactloze scanner of betaalautomaat of -proces, gebruikt door een Kaartaccepterend Bedrijf om autorisatie te verkrijgen of Transactiegegevens te verzamelen, of beide.

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.

Portal, De betekent het rapportagesysteem verstrekt door de beheerder van het PCI-programma van American Express, aangewezen door American Express. Kaartaccepterende Bedrijven en Serviceproviders zijn verplicht De Portal te gebruiken om PCI-valideringsdocumentatie bij American Express in te dienen.

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.

Primair rekeningnummer (PAN) heeft de betekenis die eraan wordt gegeven in de dan geldende Verklarende Woordenlijst voor de PCI DSS.

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

Programma, Het betekent het PCI-nalevingsprogramma van American Express.

Programma voor verbeteringen van beveiligingstechnologie (Security Technology Enhancement Programme, STEP) is het American Express-programma waarin Kaartaccepterende Bedrijven worden aangemoedigd om technologieën in te zetten die de gegevensbeveiliging verbeteren.

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.

Serviceprovider betekent een geautoriseerde verwerker, externe verwerker, gatewayleverancier, integrator van POS-systemen of een andere entiteit die aan Kaartaccepterende Bedrijven van POS-systemen of andere oplossingen of diensten 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.

Targeted Analysis Programme (TAP) betekent een programma voor vroegtijdige identificatie van een mogelijke compromittering van kaarthoudergegevens in uw Omgeving van Kaarthoudergegevens (CDE). Zie Paragraaf 1, "Targeted Analysis Programme (TAP)".

Token betekent het cryptografische token dat het PAN vervangt, gebaseerd op een gegeven index voor een onvoorspelbare waarde.

Transactie betekent een Charge of Creditering die met een Kaart wordt voltooid.

Uitgever betekent elke Entiteit (inclusief American Express en haar Gelieerde Ondernemingen) die een vergunning heeft gekregen van American Express of een Gelieerde Onderneming van American Express om Kaarten uit te geven en zich bezig te houden met de uitgifte van Kaarten.

Verklaring 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.

Verklaring 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.

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 Driemaandelijkse netwerkscans, of de Jaarlijkse verklaring van beveiligingstoetsing op locatie van het Programma voor verbeteringen van beveiligingstechnologie.