American Express®
Data Security Operating Policy – Nederland

Als toonaangevende onderneming op het vlak van consumentenbescherming legt American Express zich er reeds lang op toe Kaarthouderinformatie te beschermen om ervoor zorg te dragen dat deze informatie veilig blijft.

Gecompromitteerde gegevens hebben een negatieve invloed op consumenten, Handelaren, Serviceproviders en kaartuitgevende bedrijven. Zelfs één incident kan de reputatie van een onderneming ernstige schade toebrengen en haar mogelijkheden tot effectieve bedrijfsvoering beperken. Het aanpakken van dit risico door een beveiligingsbeleid te implementeren, kan helpen het consumentenvertrouwen en de winstgevendheid te vergroten en de reputatie van een onderneming te verbeteren.

*American Express weet dat onze Handelaren en Serviceproviders (gezamenlijk **u**) onze zorgen delen en vereist, als onderdeel van uw verantwoordelijkheden, dat u zich houdt aan de bepalingen betreffende gegevensbeveiliging in uw Overeenkomst voor de acceptatie (voor Handelaren) of de verwerking (voor Serviceproviders) van de American Express®-kaart (voor beide respectievelijk de **Overeenkomst**) en deze Data Security Operating Policy, die we mogelijk van tijd tot tijd aanpassen. Deze vereisten gelden voor al uw apparatuur, systemen en netwerken waarop Coderingssleutels, Kaarthouderinformatie en/of Gevoelige verificatiegegevens worden opgeslagen, verwerkt of verzonden.*

Termen die hier met een hoofdletter worden geschreven zonder bijgaande definitie, hebben de betekenis die daaraan wordt toegekend in de woordenlijst opgenomen aan het einde van dit beleid .

Paragraaf 1 – Normen voor de beveiliging van Coderingssleutels, Kaarthouderinformatie en Gevoelige verificatiegegevens

U moet, en u moet ervoor zorgen dat alle Gedekte partijen:

- Kaarthouderinformatie alleen opslaan ter vereenvoudiging van American Express-kaarttransacties conform en zoals vereist door de Overeenkomst; en
- voldoen aan de huidige versie van de Payment Card Industry Data Security Standard (***PCI DSS***) en de PCI PIN Security Requirements, en dan niet later dan de ingangsdatum van de implementatie van die versie; en
- alleen door de PCI goedgekeurde nieuwe of vervangende Pinapparaten en/of Betaaltoepassingen gebruiken.

U dient alle American Express-Betalingsoverzichten en kredietoverzichten te beschermen die conform de Overeenkomst worden behouden in overeenstemming met deze bepalingen betreffende gegevensbeveiliging; 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 zowel financieel als anderszins aansprakelijk tegenover American Express om ervoor te zorgen dat uw Gedekte partijen zich houden aan deze bepalingen voor gegevensbeveiliging (naast aantonen dat uw Gedekte partijen zich aan dit beleid houden, zoals wordt beschreven bij Paragraaf 4 hieronder).

Paragraaf 2 – Verplichtingen omtrent beheer van Gegevensincidenten

U dient American Express onmiddellijk op de hoogte te stellen en in geen geval later dan vierentwintig (24) uur nadat het Gegevensincident is ontdekt.

Om American Express op de hoogte te stellen, neemt u contact op met het American Express Enterprise Incident Response Program (*EIRP*). Dit kan telefonisch via +1 (602) 537-3021 ('+' duidt het IDD-voorvoegsel (International Direct Dial) aan; internationale belkosten gelden) of per e-mail via EIRP@aexp.com. U moet bij een dergelijk Gegevensincident iemand aanwijzen als contactpersoon.

- U dient elk Gegevensincident te onderwerpen aan een grondig forensisch onderzoek. In geval van een Gegevensincident waarmee 10.000 of meer unieke American Express-kaartrekeningnummers zijn gemoeid (of op verzoek van American Express), dient dit onderzoek te worden uitgevoerd door een PCI Forensic Investigator (***PFI***).
- U dient American Express direct te voorzien van alle Gecompromitteerde kaartnummers en het rapport

van het forensisch onderzoek van het gegevensincident.

- U dient met American Express samen te werken om alle problemen ten gevolge van een Gegevensincident recht te zetten. Dit houdt onder meer in dat met American Express moet worden overlegd over uw communicatie met American Express-Kaarthouders op wie het Gegevensincident betrekking heeft; bovendien moet u aan American Express alle relevante informatie verstrekken (en enige noodzakelijke verklaringen van afstand verkrijgen) om te verifiëren dat u toekomstige Gegevensincidenten kunt voorkomen op een wijze die in overeenstemming is met deze Overeenkomst.

Rapporten van forensisch onderzoek moeten de volgende informatie bevatten: forensische overzichten, nalevingsrapporten en alle andere informatie die betrekking heeft op het Gegevensincident. Bovendien moet in de rapporten de oorzaak van het Gegevensincident worden geïdentificeerd, moet worden vastgesteld of u ten tijde van het Gegevensincident hebt gehandeld conform de PCI DSS en moet worden geverifieerd dat u in de toekomst Gegevensincidenten kunt voorkomen door een plan op te nemen voor het oplossen van tekortkomingen op het vlak van PCI DSS. Op verzoek van American Express moet u zorgen voor bevestiging door een Qualified Security Assessor (*QSA*) dat de tekortkomingen zijn opgelost.

Onverminderd enige andersluidende verplichting met betrekking tot vertrouwelijkheid in de Overeenkomst heeft American Express het recht informatie over een Gegevensincident openbaar te maken aan American Express-Kaarthouders en -uitgevers, andere deelnemers van het American Express-netwerk en aan de buitenwereld, zoals vereist door toepasselijke wetgeving of door een juridisch(e), administratief(-ve) of wettelijk(e) bevel, verordening, dagvaarding, verzoek of ander proces om het risico van fraude, andere schade of anderszins zo klein mogelijk te maken, voor zover van toepassing op het gebruik van het American Express-netwerk.

PARAGRAAF 3 – SCHADELOOSSTELLINGSVERPLICHTINGEN VOOR EEN GEGEVENSINCIDENT

Uw schadeloosstellingsverplichtingen voor Gegevensincidenten richting American Express worden in de Overeenkomst bepaald in deze Paragraaf 3, zonder afstand te nemen van andere rechten en rechtsmiddelen van American Express.

American Express vereist geen schadeloosstelling van u indien het Gegevensincident (a) minder dan 10.000 unieke Gecompromitteerde kaartnummers betreft of (b):

- u American Express op de hoogte hebt gesteld van het Gegevensincident conform Paragraaf 2 van dit beleid,
- u ten tijde van het Gegevensincident hebt gehandeld conform de PCI DSS (zoals vastgesteld in het onderzoek van het Gegevensincident door de PFI) en
- het Gegevensincident niet is veroorzaakt door onbillijk gedrag van u of uw Gedekte partijen.

De schadeloosstellingsberekeningen staan in Bijlage A, aan het einde van dit document.

PARAGRAAF 4 – BELANGRIJK! PERIODIEKE VALIDERING VAN UW SYSTEMEN

U moet de volgende stappen nemen om in overeenstemming met de PCI DSS jaarlijks en elk kwartaal de status te valideren van uw apparatuur, systemen en/of netwerken (en de onderdelen daarvan) waarop Kaarthouderinformatie of Gevoelige verificatiegegevens worden opgeslagen, verwerkt of verzonden, zoals hieronder wordt beschreven.

Er zijn vier stappen vereist voor een volledige validering:

Stap 1 – Meedoen met een nalevingsprogramma van American Express conform dit beleid

Stap 2 – Uw niveau en valideringsvereisten vaststellen

Stap 3 – Vaststellen welke Valideringsdocumentatie u moet verzenden naar American Express

Stap 4 – De Valideringsdocumentatie verzenden naar American Express

Stap 1 – Meedoen met een nalevingsprogramma van American Express conform dit beleid

Handelaren van niveau 1, Handelaren van niveau 2, Handelaren van niveau 3 die American Express heeft aangewezen (zoals hieronder beschreven), Handelaren van EMV-niveau en alle Serviceproviders, zoals hieronder beschreven, moeten conform dit beleid meedoen met het nalevingsprogramma van American Express door de volledige naam, het e-mailadres, het telefoonnummer en het fysieke postadres te verstrekken van een persoon die als algemeen contactpersoon voor gegevensbeveiliging zal dienen. U dient deze informatie in te dienen bij Trustwave, het bedrijf dat het programma namens American Express uitvoert, middels een van de methoden onder Stap 4 hieronder. U dient Trustwave op de hoogte te stellen indien deze informatie verandert, en waar van toepassing bijgewerkte informatie verstrekken.

American Express kan mogelijk van bepaalde Handelaren van niveau 3 vereisen dat zij meedoen met het nalevingsprogramma van American Express conform dit beleid door hen een schriftelijke kennisgeving te sturen. De Aangewezen Handelaar van niveau 3 moet zich binnen 90 dagen vanaf ontvangst van de kennisgeving inschrijven.

Stap 2 – Uw niveau en valideringsvereisten vaststellen

Er zijn vijf niveaus voor Handelaren en twee niveaus voor Serviceproviders. De meest niveaus zijn gebaseerd op het aantal American Express-kaarttransacties. Voor een Handelaar is dit het opgetelde volume dat is ingediend door diens vestigingen, dat op het hoogste rekeningniveau van de American Express-Handelaar wordt samengevoegd. U behoort tot een van de niveaus van de onderstaande tabellen voor Handelaren en Serviceproviders.

Vereisten voor Handelaren

Voor Handelaren (niet voor Serviceproviders) zijn er vijf mogelijke classificeringen voor het niveau en de valideringsvereisten. Zodra u het Handelarenniveau hebt vastgesteld aan de hand van de onderstaande lijst, raadpleegt u de Handelarentabel om de documentatievereisten voor validering vast te stellen.

Handelaar van niveau 1 – 2,5 miljoen of meer American Express-kaarttransacties per jaar; of een Handelaar die naar het oordeel van American Express onder niveau 1 valt.

Handelaar van niveau 2 – 50.000 tot 2,5 miljoen American Express-kaarttransacties per jaar

Handelaar van niveau 3 (aangewezen) – Minder dan 50.000 American Express-kaarttransacties per jaar en door American Express aangewezen als Handelaar die valideringsdocumenten moet indienen. Aangewezen Handelaren worden door American Express ten minste 90 dagen voordat de documenten moeten zijn ingediend, schriftelijk op de hoogte gesteld.

Handelaar van niveau 3 (niet aangewezen) – Minder dan 50.000 American Express-kaarttransacties per jaar en niet door American Express aangewezen als Handelaar die valideringsdocumenten moet indienen.

Handelaar van EMV-niveau – Handelaar die in de afgelopen 12 maanden niet betrokken is geweest bij een Gegevensincident en die aan de volgende kenmerken voldoet:

- verwerkt 50.000 of meer American Express-kaarttransacties per jaar;
- ten minste 75% van alle transacties wordt uitgevoerd door een Kaarthouder die de fysieke kaart bij zich heeft; en
- deze uitgevoerde transacties zijn afkomstig van EMV-Chipapparaten.

Handelarentabel

Niveau (hier-boven gedefinieerd)	Validering Documentatie (gedefinieerd in Stap 3 hieronder)	Vereiste
1	• Jaarlijks rapport van beveiligingsbeoordeling op locatie • Driemaandelijkse netwerkscan	Verplicht
2	• Jaarlijkse enquête voor zelfbeoordeling • Driemaandelijkse netwerkscan	Verplicht
3 Aangewezen	• Jaarlijkse enquête voor zelfbeoordeling • Driemaandelijkse netwerkscan	Verplicht
3*	• Jaarlijkse enquête voor zelfbeoordeling • Driemaandelijkse netwerkscan	Sterk aanbevolen
EMV**	• Geprioriteerde aanpaksamenvatting en Attest van naleving van de PCI DSS	Verplicht

*Om twijfel te voorkomen: Handelaren van niveau 3 (met uitzondering van Aangewezen Handelaren van niveau 3) hoeven geen Valideringsdocumentatie in te dienen, maar moeten voldoen en zijn onderhevig aan en aansprakelijk voor alle andere bepalingen van deze Data Security Operating Policy.

**EMV-niveau is niet beschikbaar voor Handelaren bij wie in de twaalf (12) maanden voorafgaand aan de datum van de jaarlijkse nalevingsbeoordeling een Gegevensincident heeft plaatsgevonden.

Vereisten voor Serviceproviders

Voor Serviceproviders (niet voor Handelaren) zijn er twee mogelijke classificeringen voor het niveau en de valideringsvereisten. Zodra u het Serviceproviderniveau hebt vastgesteld aan de hand van de onderstaande lijst, raadpleegt u de Serviceprovidertabel om de documentatievereisten voor validering vast te stellen.

Serviceprovider van niveau 1 – 2,5 miljoen of meer American Express-kaarttransacties per jaar; of een Serviceprovider die naar het oordeel van American Express onder niveau 1 valt.

Serviceprovider van niveau 2 – minder dan 2,5 miljoen American Express-kaarttransacties per jaar; en elke andere Serviceprovider die naar het oordeel van American Express niet onder niveau 1 valt.

Serviceprovidertabel

Niveau (hierboven gedefinieerd)	Validering Documentatie (gedefinieerd in Stap 3 hieronder)	Vereiste
1	• Jaarlijks rapport van beveiligingsbeoordeling op locatie • Driemaandelijkse netwerkscan	Verplicht
2	• Jaarlijkse enquête voor zelfbeoordeling • Driemaandelijkse netwerkscan	Verplicht

Stap 3 – Vaststellen welke Valideringsdocumentatie u moet verzenden naar American Express

De volgende documenten zijn verplicht voor verschillende niveaus van Handelaren en Serviceproviders, zoals weergegeven in de Handelarentabel en Serviceprovidertabel hierboven.

Jaarlijkse beveiligingsbeoordeling op locatie – De jaarlijkse beveiligingsbeoordeling op locatie is een gedetailleerde inspectie op locatie van uw apparatuur, systemen en netwerken (en de onderdelen daarvan) waarop Kaarthouderinformatie en/of Gevoelige verificatiegegevens worden opgeslagen, verwerkt of verzonden. De beoordeling moet worden uitgevoerd door

- een QSA of
- u en officieel worden bevestigd door uw Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer of Principal Officer en jaarlijks worden ingediend bij American Express voor het desbetreffende Attest van naleving (***AOC***, Attestation of Compliance).

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

Jaarlijkse enquête voor zelfbeoordeling – De Jaarlijkse enquête voor zelfbeoordeling is een proces waarbij de PCI DSS Self-Assessment Questionnaire (***SAQ***) wordt gebruikt en waarmee u zelf een inspectie kunt uitvoeren van uw apparatuur, systemen en netwerken (en de onderdelen daarvan) waarop Kaarthouderinformatie en/of Gevoelige verificatiegegevens worden opgeslagen, verwerkt of verzonden. Deze beoordeling moet worden uitgevoerd door u en officieel worden bevestigd door uw Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer of Principal Officer. Het AOC-gedeelte van de SAQ moet jaarlijks worden ingediend bij American Express. Het AOC-gedeelte van de SAQ moet de naleving aantonen van alle vereisten van de PCI DSS en op verzoek kopieën bevatten van de volledige SAQ (Handelaren van niveau 2, alle Handelaren van niveau 3 en Serviceproviders van niveau 2).

Driemaandelijkse netwerkscan – De Driemaandelijkse netwerkscan is een proces waarmee op afstand uw met internet verbonden computernetwerken en webservers worden getest op potentiële zwaktes en kwetsbaarheden. Deze moet worden uitgevoerd door een Goedgekeurde scanprovider (***ASV***, Approved Scanning Vendor). U moet elk kwartaal het Scanrapport met attest van naleving van scanregels van de ASV (***AOSC***, Attestation of Scan Compliance) of de executive summary van de bevindingen van de scan (en op aanvraag kopieën van de volledige scan) voltooien en indienen bij American Express. De AOSC of executive summary moet aantonen 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 Handelaren, behalve EMV-niveau; alle Serviceproviders).

Jaarlijkse beoordeling van nalevingsmijlpalen 1-4 van de valideringsdocumentatie van de geprioriteerde aanpak van de PCI DSS – De Jaarlijkse beoordeling van nalevingsmijlpalen 1-4 van de valideringsdocumentatie van de geprioriteerde aanpak van de PCI DSS is een inspectie van uw apparatuur, systemen en netwerken (en de onderdelen daarvan) waarop Kaarthouderinformatie en/of Gevoelige verificatiegegevens worden opgeslagen, verwerkt of verzonden. Deze moet worden uitgevoerd door u en officieel worden bevestigd door uw Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer of Principal Officer en jaarlijks worden ingediend bij American Express voor de Geprioriteerde aanpaksamenvatting en Attest van naleving van de PCI DSS (***PASAOC***, Prioritized Approach Summary & Attestation of Compliance). De PASAOC moet de naleving aantonen van de Mijlpalen 1-4 van de Geprioriteerde aanpak van de PCI DSS en moet, op verzoek, de volledige details van deze naleving bevatten. (Alleen Handelaren van EMV-niveau).

Geen naleving van de PCI DSS – Als u niet voldoet aan de PCI DSS, moet u een AOC invullen, inclusief "Deel 4. Actieplan in geval van niet-naleving" en een datum opgeven waarop de problemen zijn verholpen; deze datum moet voor succesvolle naleving binnen twaalf maanden van de datum van het AOC liggen. U dient dit AOC inclusief "Actieplan in geval van niet-naleving" in te dienen bij American Express middels een van de methoden onder Stap 4 hieronder. U dient American Express periodiek op de hoogte te houden van uw

voortgang met betrekking tot het oplossen van de niet-naleving in overeenstemming met het "Actieplan in geval van niet-naleving" (Handelaren van niveau 1, Handelaren van niveau 2 en Aangewezen Handelaren van niveau 3; alle Serviceproviders).

American Express legt u geen boetes voor niet valideren op (zoals hieronder beschreven) voor zover het niet naleven betrekking heeft op de periode vóór de gestelde oplossingsdatum. U blijft echter aansprakelijk tegenover American Express voor alle schadeloosstellingsverplichtingen voor een Gegevensincident en u bent onderhevig aan alle andere bepalingen in dit beleid.

Stap 4 – De Valideringsdocumentatie verzenden naar American Express

Handelaren van niveau 1, Handelaren van niveau 2, Aangewezen Handelaren van niveau 3, Handelaren van EMV-niveau en alle Serviceproviders moeten de Valideringsdocumentatie indienen die in de tabellen bij Stap 2 zijn gemarkeerd als 'Verplicht'.

U dient uw Valideringsdocumentatie volgens een van de volgende methoden in te dienen bij Trustwave:

Veilige portal: Valideringsdocumentatie kan worden geüpload via de veilige portal van Trustwave op https://login.trustwave.com.

Neem voor instructies voor het gebruik van deze portal contact op met Trustwave via het telefoonnummer + 800 9000 1140 of +1 (312) 267-3208 of via het e-mailadres AmericanExpressCompliance@trustwave.com.

Veilige fax: Valideringsdocumentatie kan per fax worden verzonden naar: +1 (312) 276-4019. ('+' duidt het IDD-voorvoegsel (International Direct Dial) aan; internationale belkosten gelden). Geef uw naam, bedrijfsnaam, de naam van uw contactpersoon voor gegevensbeveiliging, uw adres en telefoonnummer op. Handelaren dien ook hun 10-cijferige American Express Merchant-nummer op te geven.

Als u vragen hebt over het programma of het bovenstaande proces, neemt u contact op met Trustwave via het telefoonnummer + 800 9000 1140 of +1 (312) 267-3208 of via het e-mailadres AmericanExpressCompliance@trustwave.com.

Naleving en validering geschieden op uw kosten. Door Valideringsdocumentatie in te dienen geeft u aan en garandeert u American Express dat u gemachtigd bent de informatie daarin bekend te maken en dat u de Valideringsdocumentatie aan American Express verstrekt zonder de rechten van derden te schenden.

Boetes en beëindiging van de Overeenkomst bij niet valideren

American Express heeft het recht u boetes op te leggen voor niet valideren en de Overeenkomst te beëindigen als u niet voldoet aan deze vereisten of niet vóór de gestelde deadline de verplichte Valideringsdocumentatie verstrekt aan American Express. American Express stelt u afzonderlijk op de hoogte van de deadlines voor elke jaarlijkse en driemaandelijkse rapportageperiode.

Beschrijving (Valuta: EUR (€))	Handelaar of Serviceprovider van niveau 1	Handelaar of Serviceprovider van niveau 2, Handelaar van EMV-niveau	Alleen Aangewezen Handelaren van niveau 3
Er wordt een boete voor niet valideren vastgesteld als de Valideringsdocumentatie niet wordt ontvangen voor de eerste deadline.	€19.000	€4.000	€15
Er wordt een extra boete voor niet valideren vastgesteld als de Valideringsdocumentatie niet wordt ontvangen binnen 30 dagen na de eerste deadline.	€26.000	€7.500	
Er wordt een extra boete voor niet valideren vastgesteld als de Valideringsdocumentatie niet wordt ontvangen binnen 60 dagen na de eerste deadline.	€34.000	€11.000	

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

Paragraaf 5 – Vertrouwelijkheid

American Express zal redelijke maatregelen treffen om gedurende een periode van drie jaar vanaf de ontvangstdatum uw nalevingsrapporten, inclusief de Valideringsdocumentatie, vertrouwelijk te houden (en ervoor te zorgen dat agenten en onderaannemers van American Express, inclusief Trustwave, dat ook doen) en de Valideringsdocumentatie niet openbaar te maken aan een derde partij (anders dan gelieerde bedrijven, agenten, vertegenwoordigers, Serviceproviders en onderaannemers van American Express). Deze vertrouwelijkheidsverplichting geldt niet op Valideringsdocumentatie die:

i. al vóór bekendmaking bekend was bij American Express;
ii. zonder inbreuk van deze paragraaf door American Express openbaar toegankelijk is of wordt;
iii. door American Express rechtmatig is ontvangen van een derde partij zonder vertrouwelijkheidsverplichting;
iv. onafhankelijk is ontwikkeld door American Express; of
v. verplicht bekend moet worden gemaakt wegens een gerechtelijk bevel, bevel van een overheidsinstantie, wegens een wet, regel, dagvaarding, verzoek voor inzage van stukken, sommering of ander bestuursproces of juridische proces of wegens een formeel of informeel onderzoek door een overheidsinstantie (inclusief toezichthouders, inspecteurs of wetshandhavingsinstanties).

Paragraaf 6 – Disclaimer

AMERICAN EXPRESS DOET HIERBIJ AFSTAND VAN ALLE VOORSTELLINGEN VAN ZAKEN, GARANTIES EN AANSPRAKELIJKHEDEN MET BETREKKING TOT DEZE DATA SECURITY OPERATING POLICY, DE PCI DSS, DE EMV-SPECIFICATIES EN DE AANDUIDING EN PRESTATIES VAN QSA's, ASV's EN PFI's, ZOWEL UITDRUKKELIJK, IMPLICIET, KRACHTENS DE WET ALS ANDERSZINS, INCLUSIEF ENIGE GARANTIE MET BETREKKING TOT DE VERHANDELBAARHEID OF GESCHIKTHEID VOOR EEN SPECIFIEK DOEL. UITGEVERS VAN AMERICAN EXPRESS-KAARTEN ZIJN IN DIT BELEID GEEN BEGUNSTIGDEN.

Nuttige websites

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

PCI Security Standards Council, LLC:

http://www.pcisecuritystandards.org

BIJLAGE A: SCHADELOOSSTELLINGSBEREKENINGEN

U bent als volgt aansprakelijk voor alle Gegevensincidenten. Voor een Gegevensincident dat zich beperkt tot American Express-kaartrekeningnummers, moet u American Express direct compenseren door een boete te betalen voor niet-naleving met betrekking tot het Gegevensincident, waarbij een maximum geldt van USD 100.000 per Gegevensincident. Voor een Gegevensincident waarmee American Express-kaartrekeningnummers met Gevoelige verificatiegegevens zijn gemoeid, moet u American Express direct compenseren voor:

- incrementele fraude (hieronder gedefinieerd) binnen de Gegevensincidentperiode en
- kosten voor controle en vervanging van kaarten à (i) USD 1,00 per kaartrekeningnummer voor 90% van het totale aantal Gecompromitteerde kaartnummers en (ii) USD 5,00 per kaartrekeningnummer voor 10% van het totale aantal Gecompromitteerde kaartnummers en
- een boete voor niet-naleving met betrekking tot een Gegevensincident, waarvoor een maximumboete van USD 100,000 per Gegevensincident geldt.

American Express zal 'incrementele fraude' met de volgende methode berekenen:

Incrementele fraude = (X – Y) keer Z, waarbij:

X =
- totale fraudeverliezen van kaartuitgevers, exclusief frauduleuze restitutie en verlies door frauduleuze kaarttoepassingen met Gecompromitteerde kaartnummers gedurende de Gegevensincidentperiode gedeeld door
- het totale Betalingsvolume van kaartuitgevers met Gecompromitteerde kaartnummers gedurende de Gegevensincidentperiode.

Y =
- totale fraudeverliezen van kaartuitgevers, exclusief frauduleuze restitutie en verlies door frauduleuze American Express-kaarttoepassingen met niet-Gecompromitteerde kaartnummers gedurende de Gegevensincidentperiode gedeeld door
- het totale Betalingsvolume van kaartuitgevers met niet-Gecompromitteerde kaartnummers gedurende de Gegevensincidentperiode.

Z = het totale Betalingsvolume van kaartuitgevers met Gecompromitteerde kaartnummers gedurende de Gegevensincidentperiode.

American Express telt bij de berekening van incrementele fraude en kosten voor controle en vervanging van kaarten geen American Express-kaartrekeningnummers mee die betrokken waren bij een ander Gegevensincident met American Express-kaartrekeningnummers met Gevoelige verificatiegegevens, mits American Express binnen twaalf (12) maanden vóór de Notificatiedatum op de hoogte is gesteld van het andere Gegevensincident. Alle berekeningen die American Express met deze methodologie maakt zijn definitief.

Schadeloosstellingsverplichtingen van Handelaren voor Gegevensincidenten zoals hierin bepaald, worden niet beschouwd als incidentele schade, indirecte schade, speculatieve schade, gevolgschade, speciale schade, schade door strafmaatregelen of smartengeld op grond van deze Overeenkomst, mits dergelijke verplichtingen geen schade omvatten die is gerelateerd aan of de aard heeft van inkomsten- of winstderving, verlies van goodwill of verlies van zakelijke kansen.

BIJLAGE B: WOORDENLIJST

Uitsluitend voor dit beleid zijn de volgende definities van toepassing:

American Express-kaart (of Kaart)

- elk(e) kaart, apparaat voor rekeningtoegang of betaalapparaat of -service met de naam, het logo, het handelsmerk, het dienstmerk, de handelsnaam of andere bedrijfseigen ontwerpen of aanduidingen van American Express of een van diens gelieerde bedrijven die/dat is uitgegeven door een uitgever of
- een kaartrekeningnummer

Attest van naleving (of AOC) betekent een verklaring over de status van uw naleving van de PCI DSS in de vorm die is bepaald door de Payment Card Industry Security Standards Council, LLC.

Goedgekeurde scanprovider (of ASV) betekent een entiteit die volgens de Payment Card Industry Security Standards Council, LLC gekwalificeerd is voor de validering van naleving van specifieke PCI DSS-vereisten door kwetsbaarheidsscans uit te voeren op omgevingen die in contact staan met internet.

Attest van naleving van scanregels (of AOSC) betekent een verklaring over de status van uw naleving van de PCI DSS op basis van een netwerkscan in de vorm die is bepaald door de Payment Card Industry Security Standards Council, LLC.

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

Kaarthouder betekent een persoon of entiteit (i) die of dat een overeenkomst is aangegaan waarin een kaartrekening is gemaakt bij een uitgever of (ii) wiens naam op de kaart staat.

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

Betaling betekent een betaling of aankoop die met de kaart wordt gedaan.

Chip betekent een microchip die in de kaart is geïntegreerd en die Kaarthouderinformatie en rekeninginformatie bevat.

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

Chipapparaat betekent een apparaat op een Point of Sale met een geldige en actuele EMVCo-goedkeuring/-certificering (www.emvco.com) dat voor AEIPS geschikte transacties met Chipkaarten kan verwerken.

Gecompromitteerd kaartnummer betekent een American Express-kaartrekeningnummer dat betrokken is bij een Gegevensincident.

Gedekte partijen betekent al uw werknemers, agenten, vertegenwoordigers, onderaannemers, Processors, Serviceproviders, leveranciers van uw Point of Sale-apparatuur of -systemen of oplossingen voor de verwerking van betalingen, plus elke andere partij die u toegang tot Kaarthouderinformatie geeft conform de Overeenkomst.

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

Gegevensincident betekent een incident waarbij Coderingssleutels van American Express zijn betrokken, of ten minste één American Express-kaartrekeningnummer waarbij sprake is van:

- ongeautoriseerd(e) toegang of gebruik van Kaarthouderinformatie en/of Gevoelige verificatiegegevens die worden opgeslagen, verwerkt of verzonden op uw apparatuur, systemen en/of netwerken (of de onderdelen daarvan);
- gebruik van deze Kaarthouderinformatie en/of Gevoelige verificatiegegevens dat niet in overeenstemming is met de Overeenkomst; en/of
- vermoed(e) of bevestigd(e) verlies, diefstal of verduistering op welke wijze dan ook van enige media, materialen, records of informatie die deze Kaarthouderinformatie en/of Gevoelige verificatiegegevens bevatten.

Gegevensincidentperiode betekent de periode vanaf 365 dagen vóór de Notificatiedatum tot 30 dagen na de Notificatiedatum.

Aangewezen Handelaar van niveau 3 betekent een Handelaar die er door American Express van op de hoogte is gesteld dat hij/zij moet deelnemen aan het PCI-nalevingsprogramma van American Express en de nalevingsstatus moet rapporteren.

EMV-specificaties betekent de specificaties die zijn uitgegeven door EMVCo, LLC; deze zijn beschikbaar op http://www.emvco.com.

EMV-transactie betekent een transactie met een chipkaart (ook wel 'IC-kaart', 'integrated circuit card', '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. Goedgekeurde EMV-typen vindt u op http://www.emvco.com.

Coderingssleutel (Coderingssleutel van American Express) **betekent** een sleutel die wordt gebruikt bij het verwerken, genereren, laden en/of beveiligen van rekeninggegevens. Dit omvat maar is niet beperkt tot:

- Sleutelcoderingssleutels (KEK's, Key Encryption Keys): zonehoofdsleutels (ZMK's, Zone Master Keys) en zonepincodesleutels (ZPK's, Zone PIN Keys)
- Hoofdsleutels die worden gebruikt in veilige cryptografische apparaten: Lokale hoofdsleutels (LMK's, Local Master Keys)
- Kaartbeveiligingscodesleutels (CSCK's, Card Security Code Keys)
- Pincodesleutels: basisderivatiesleutels (BDK's, Base Derivation Keys), pincodecoderingssleutels (PEK's, PIN Encryption Key) en ZPK's

Handelaar van niveau 1 – 2,5 miljoen of meer American Express-kaarttransacties per jaar; of een Handelaar die naar het oordeel van American Express onder niveau 1 valt.

Handelaar van niveau 2 – 50.000 tot 2,5 miljoen American Express-kaarttransacties per jaar

Handelaar van niveau 3 – Minder dan 50.000 American Express-kaarttransacties per jaar en niet door American Express aangewezen.

Handelaar van niveau 3 (aangewezen) betekent een Handelaar die er door American Express van op de hoogte is gesteld dat hij/zij moet deelnemen aan het PCI-nalevingsprogramma van American Express en de nalevingsstatus moet rapporteren.

Serviceprovider van niveau 1 – 2,5 miljoen of meer American Express-kaarttransacties per jaar; of een Serviceprovider die naar het oordeel van American Express onder niveau 1 valt.

Serviceprovider van niveau 2 – minder dan 2,5 miljoen American Express-kaarttransacties per jaar; en elke andere Serviceprovider die naar het oordeel van American Express niet onder niveau 1 valt.

Handelaar van EMV-niveau – Handelaar die in de afgelopen 12 maanden niet betrokken is geweest bij een Gegevensincident en die aan de volgende kenmerken voldoet:

- Verwerkt 50.000 of meer American Express-kaarttransacties per jaar.
- Ten minste 75% van de transacties van de Handelaar wordt uitgevoerd met de fysieke kaart en is afkomstig van Point of Sale-systemen die voldoen aan de EMV-specificaties van American Express.

Mijlpalen 1-4 betekent de prioriteiten die aan PCI DSS-vereisten zijn toegewezen door de Geprioriteerde aanpak van de PCI, die beschikbaar is op https://www.pcisecuritystandards.org.

Notificatiedatum betekent een door American Express vastgestelde datum waarop uitgevers een melding ontvangen van het Gegevensincident.

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 https://www.pcisecuritystandards.org.

Door de PCI goedgekeurd betekent dat een Pinapparaat en/of Betaaltoepassing ten tijde van het gebruik op de lijst staat met goedgekeurde bedrijven en leveranciers die wordt onderhouden door de PCI Security Standards Council, LLC; deze is beschikbaar op https://www.pcisecuritystandards.org.

PCI DSS staat voor de Payment Card Industry Data Security Standard; deze is beschikbaar op https://www.pcisecuritystandards.org.

Geprioriteerde aanpak van de PCI DSS geeft aan het PCI DSS-document dat beschikbaar is op https://www.pcisecuritystandards.org/security_standards/prioritized.php.

Geprioriteerde aanpaksamenvatting en Attest van naleving van de PCI DSS (PASAOC) betekent een verklaring over de status van uw naleving van de Geprioriteerde aanpak van de PCI DSS in de vorm die is bepaald door de Payment Card Industry Security Standards Council, LLC.

PCI Forensic Investigator (PFI) betekent een entiteit die is goedgekeurd door de Payment Card Industry Security Standards Council, LLC voor het uitvoeren van forensisch onderzoek naar een lek of gecompromitteerde betaalkaartgegevens.

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

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

Processor betekent een Serviceprovider voor Handelaren die verwerking van autorisatie en indiening biedt aan het American Express-netwerk.

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

Enquête voor zelfbeoordeling (SAQ) betekent een hulpmiddel voor zelfbeoordeling dat is ontwikkeld door de Payment Card Industry Security Standards Council, LLC en dat is bestemd voor het evalueren en attesteren van naleving van de PCI DSS.

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

Serviceprovider betekent een geautoriseerde Processor, externe Processor, gatewayleverancier of een andere entiteit die aan Handelaren Point of Sale-apparatuur, -software of -systemen of andere oplossingen of services voor de verwerking van betalingen levert.

Transactie betekent een Betaling of Krediet die of dat wordt voltooid met een kaart.

Valideringsdocumentatie betekent het AOC dat is opgesteld in verband met een jaarlijkse beveiligingsbeoordeling ter plekke of SAQ, het AOSC en executive summary's van de bevindingen die zijn opgesteld in verband met Driemaandelijkse netwerkscans of het jaarlijkse EMV-attest.