AMERICAN EXPRESS

Politique de sécurité des données (DSOP)

AMERICAN EXPRESS

Récapitulatif des modifications de la DSOP

Icônes

Les mises à jour majeures sont indiquées dans le Tableau récapitulatif des modifications, ainsi que dans la *DSOP* par une barre de modification. Une barre de modification est une ligne verticale, généralement située dans la marge de gauche, qui identifie les ajouts ou révisions de texte. Seuls les changements importants dans la *DSOP* pouvant avoir des répercussions sur les procédures opérationnelles des Commerçants sont indiqués par une barre de modification similaire à celle qui figure dans la marge de gauche.

Le texte supprimé est marqué à l'aide d'une icône de corbeille située dans la marge à côté de toute suppression importante de texte, y compris de sections, tableaux, paragraphes, remarques et points importants. Le texte supprimé est référencé dans ce Récapitulatif des modifications en utilisant la numérotation des sections issue de la publication précédente afin d'éviter toute confusion.

Les lignes bleues encadrant les paragraphes indiquent des informations spécifiques à une région donnée.

Tableau récapitulatif des modifications

Les mises à jour majeures sont indiquées dans le tableau suivant, ainsi que dans la *DSOP* par une barre de modification.

Section/Sous-section	Description de la modification
Aucune modification n'a été effectuée pour cette publication.	

Section 1 Introduction à la DSOP et aux Normes de protection

En tant que leader en matière de protection des consommateurs, American Express s'engage depuis longtemps à protéger les Données et les Données d'authentification sensibles des Titulaires de Carte, afin de garantir qu'elles sont conservées en toute sécurité.

La mise en danger de la confidentialité des données a un impact négatif sur les clients, les Commerçants, les Prestataires de services et les émetteurs de cartes. Un seul incident peut avoir des conséquences extrêmement néfastes sur la réputation d'une entreprise et nuire gravement à ses activités. En mettant en place des politiques opérationnelles de sécurité afin de lutter contre ce risque, l'entreprise peut gagner la confiance de ses clients, augmenter sa rentabilité et améliorer sa réputation.

American Express sait que vous - Commerçants et Prestataires de services (collectivement, vous) - partagez nos préoccupations et demande, dans le cadre de vos responsabilités, que **vous** respectez les dispositions concernant la sécurité des données dans le cadre de notre Contrat d'acceptation (pour les Commerçants) ou de traitement (pour les Prestataires de services) de la Carte American Express® (pour chacun, le **Contrat**) et la présente Politique de sécurité des données (DSOP), qui pourra être modifiée. Ces exigences s'appliquent à l'ensemble des équipements, systèmes et réseaux (et leurs composants) utilisés pour effectuer l'enregistrement, le traitement ou la transmission des Clés de cryptage, des Données des Titulaires de Carte ou des Données d'authentification sensibles (ou d'une combinaison d'entre elles).

Les termes en majuscules utilisés mais non définis dans la présente ont le sens qui leur est attribué dans le glossaire à la fin de cette politique.

La Politique de sécurité des données (DSOP) se compose d'un ensemble d'exigences complètes visant à protéger les Données de compte au cours de leur stockage, de leur traitement ou de leur transmission.

American Express exige que tous les Commerçants et Prestataires de services respectent la Norme de sécurité des données de l'industrie des Cartes de paiement (PCI DSS). Pour répondre à cette exigence, vous, ainsi que vos Parties assujetties, devez :

- Enregistrer les Données des Titulaires de Carte uniquement dans le but de faciliter les Transactions par Carte American Express dans le cadre du Contrat.
- Respecter la norme de sécurité des données PCI DSS et les autres exigences du Payment Card Industry Security Standards Council (Conseil des normes de sécurité de l'industrie des Cartes de paiement, PCI SSC) applicables à votre traitement, stockage ou transmission des Clés de cryptage, Données des Titulaires de Carte ou des Données d'authentification sensibles en vigueur avant la mise en œuvre effective de cette version de l'exigence applicable.
- S'assurer d'utiliser des produits approuvés par la PCI pour déployer ou remplacer la technologie de stockage, traitement ou transmission des données.

Vous devez protéger tous les Enregistrements des Débits et des Crédits d'American Express conservés en application du Contrat, conformément à ces dispositions concernant la sécurité des données ; vous devez utiliser ces enregistrements uniquement pour les besoins du Contrat et les protéger en conséquence. Vous êtes responsable, y compris financièrement, à l'égard d'American Express du respect de ces dispositions concernant la sécurité des données par vos Parties assujetties (à l'exception de la preuve du respect de la part de vos Parties assujetties de la Section 2, « Programme de conformité à la norme PCI DSS (Validation périodique importante de vos systèmes) », sauf indication contraire dans cette section). Des informations détaillées concernant les normes PCI et la conformité à leurs exigences sont disponibles sur le site www.pcisecuritystandards.org.

Section 2 Programme de conformité à la norme PCI DSS (Validation périodique importante de vos systèmes)

Vous devez prendre les mesures suivantes pour valider selon la norme PCI DSS, tous les ans et tous les 90 jours comme décrit ci-dessous, l'état de vos équipements, systèmes et/ou réseaux (et de leurs composants), ainsi que ceux de vos Franchisés, sur lesquels les Données des Titulaires de carte ou les Données d'authentification sensibles sont stockées, traitées ou transmises.

La validation comprend quatre mesures à prendre :

- Mesure 1: Participation au programme de conformité PCI d'American Express dans le cadre de cette politique.
- Mesure 2: Compréhension de votre niveau Commerçant/de Prestataire de services et des exigences à respecter en matière de documents de validation.
- Mesure 3: Réalisation des Documents de validation à envoyer à American Express.
- Mesure 4: Envoi des Documents de validation à American Express dans les délais impartis.

Mesure 1: Participation au Programme de conformité d'American Express dans le cadre de cette politique

Les Commerçants de niveau 1, de niveau 2 et tous les Prestataires de services, comme indiqué ci-dessous, doivent participer au Programme dans le cadre de cette politique. American Express pourra, à son entière discrétion, désigner des Commerçants de niveau 3 et de niveau 4 particuliers pour qu'ils participent au Programme dans le cadre de cette politique.

Les Commerçants et les Prestataires de services tenus de participer au Programme doivent s'inscrire dans le Portail fourni par l'Administrateur du Programme sélectionné par American Express dans les délais impartis.

- Vous devez accepter toutes les conditions raisonnables qui sont associées à l'utilisation du Portail.
- Vous devez assigner et fournir les coordonnées valides d'au moins une personne à contacter pour les questions de sécurité des données dans le Portail. Les informations requises comprennent:
  - Le nom complet
  - L'adresse électronique
  - Le numéro de téléphone
  - L'adresse postale physique
- Vous devez fournir les coordonnées mises à jour ou les nouvelles coordonnées de la personne à contacter pour les questions de sécurité des données dans le Portail en cas de modification de ces coordonnées.
- Vous devez vous assurer que vos systèmes soient mis à jour de manière à permettre les communications du service à partir du domaine désigné du Portail.

Votre manquement à fournir ou à mettre à jour les coordonnées actuelles de la personne à contacter pour les questions de sécurité des données ou à permettre les communications par courrier électronique n'affectera pas nos droits d'imposition de frais.

Mesure 2: Compréhension de votre niveau Commerçant/de Prestataire de service et des exigences à respecter en matière de documents de validation

Il existe quatre niveaux Commerçant applicables aux Commerçants et deux niveaux applicables aux Prestataires de services selon votre volume de Transactions de Cartes American Express.

- Pour les Commerçants, c'est le volume soumis par leurs Établissements qui se cumule au niveau du Compte Commerçant American Express le plus élevé.*
- Pour les Prestataires de services, c'est le volume total soumis par le Prestataire de services et les Entités Prestataires de services auxquelles vous fournissez des services.

Les Transactions émises par l'entreprise (Buyer Initiated Payments, BIP) ne sont pas incluses dans le volume des Transactions par Carte American Express pour déterminer le niveau Commerçant et les exigences à respecter en matière de validation. Vous entrerez dans l'un des niveaux Commerçant indiqués dans le Tableau A-1 : Niveaux Commerçant et de Prestataire de services.

* Dans le cas des Franchiseurs, cela inclut le volume provenant des Établissements de leurs Franchisés. Les Franchiseurs qui demandent à leurs Franchisés d'utiliser un Système de point de vente (POS) ou Prestataire de services spécifique doivent également fournir les Documents de validation aux Franchisés concernés.

Tableau A-1 : Niveaux Commerçant et de Prestataire de services

Niveau Commerçant	Transactions American Express annuelles
Commerçant de niveau 1	2,5 millions de Transactions de Cartes American Express ou plus par an ; ou tout Commerçant auquel American Express assigne, à sa discrétion, le niveau 1.
Commerçant de niveau 2	50 000 à moins de 2,5 millions de Transactions de Cartes American Express par an.
Commerçant de niveau 3	10 000 à moins de 50 000 Transactions de Cartes American Express par an.
Commerçant de niveau 4	Moins de 10 000 Transactions de Cartes American Express par an.
Niveau de Prestataire de services	**Transactions American Express annuelles**
Prestataire de services de niveau 1	2,5 millions de Transactions de Cartes American Express ou plus par an ; ou tout Prestataire de services qu'American Express estime être de niveau 1.
Prestataire de services de niveau 2	moins de 2,5 millions de Transactions de Cartes American Express par an ; ou tout Prestataire de services qu'American Express n'estime pas être de niveau 1.

Exigences concernant les Documents de validation Commerçants

Les Commerçants (pas les Prestataires de services) ont quatre classifications possibles de niveau Commerçant. Après avoir déterminé le niveau Commerçant dans le Tableau A-1 : Niveaux Commerçant et de Prestataire de services (ci-dessus), consultez le Tableau A-2 : Documents de validation Commerçants pour déterminer les exigences à respecter en matière de documentation de validation.

Tableau A-2 : Documents de validation Commerçants

Niveau Commerçant/ Transactions American Express annuelles	Rapport sur la conformité Attestation de conformité (ROC AOC)	Questionnaire d'autoévaluation Attestation de conformité (SAQ AOC) ET Examen trimestriel des vulnérabilités externes du réseau (Examen)	Attestation du Programme d'amélioration des technologies de la sécurité (STEP) pour les Commerçants admissibles
Niveau 1/ 2,5 millions ou plus	Obligatoire	Non applicable	Facultatif avec l'autorisation d'American Express (remplace le ROC)
Niveau 2/ 50 000 à moins de 2,5 millions	Facultatif	SAQ AOC obligatoire (à moins de soumettre un ROC AOC) ; examen obligatoire avec certains types de SAQ	Facultatif avec l'autorisation d'American Express* (remplace le SAQ et l'examen du réseau ou le ROC)
Niveau 3**/ 10 000 à moins de 50 000	Facultatif	SAQ AOC facultatif (obligatoire si American Express le demande) ; examen obligatoire avec certains types de SAQ	Facultatif avec l'autorisation d'American Express* (remplace le SAQ et l'examen du réseau ou le ROC)
Niveau 4**/ Moins de 10 000	Facultatif	SAQ AOC facultatif (obligatoire si American Express le demande) ; examen obligatoire avec certains types de SAQ	Facultatif avec l'autorisation d'American Express* (remplace le SAQ et l'examen du réseau ou le ROC)

* **Remarque :** L'équipe PCI d'American Express examinera la demande et l'admissibilité, et confirmera si vous remplissez les critères de participation au Programme STEP. Veuillez prendre contact avec votre chargé de clientèle et/ou AXPPCIComplianceProgram@aexp.com pour vérifier les conditions d'admissibilité.

**Pour éviter toute ambiguïté, les Commerçants de niveau 3 et de niveau 4 ne sont pas tenus d'envoyer les Documents de validation, sauf si cela est exigé sur appréciation d'American Express, mais doivent néanmoins respecter, et sont responsables en vertu de toutes les autres dispositions de respecter, la présente Politique de sécurité des données.

American Express se réserve le droit de vérifier l'exhaustivité, l'exactitude et le bien-fondé de vos Documents de validation PCI. American Express pourra vous demander de fournir des documents justificatifs supplémentaires

pour évaluation à cette fin. De plus, American Express a le droit de vous demander de faire appel à un Évaluateur qualifié en matière de sécurité (Qualified Security Assessor, QSA) ou à un Enquêteur judiciaire PCI (Forensic Investigator, PFI) approuvé par le PCI Security Standards Council.

Exigences concernant les Documents de validation des Prestataires de services

Les Prestataires de services (pas les Commerçants) ont deux classifications possibles de Niveau. Après avoir déterminé le niveau de Prestataire de services dans le Tableau A-1 : Niveaux Commerçant et de Prestataire de services (ci-dessus), consultez le Tableau A-3 : Documents de validation des Prestataires de services pour déterminer les exigences à respecter en matière de documentation de validation.

Les Prestataires de services ne sont pas admissibles au Programme STEP.

Tableau A-3 : Documents de validation des Prestataires de services

Niveau	Documents de validation	Exigence
1	Rapport annuel sur la conformité Attestation de conformité (ROC AOC)	Obligatoire
2	SAQ D annuel (Prestataire de services) et Examen trimestriel du réseau ou Rapport annuel sur la conformité Attestation de conformité (ROC AOC), le cas échéant	Obligatoire

Il est recommandé que les Prestataires de services se conforment également à la Validation supplémentaire par des entités désignées PCI.

Programme d'amélioration des technologies de la sécurité (STEP)

Les Commerçants respectant la norme PCI DSS peuvent, sur appréciation d'American Express, se qualifier pour le Programme d'amélioration des technologies de la sécurité (STEP) d'American Express s'ils déploient certaines technologies de sécurité supplémentaires via les environnements de traitement de leur Carte. Le Programme STEP s'applique uniquement si le Commerçant n'a pas eu d'Incident touchant les données au cours des 12 derniers mois et si 75 % de toutes les Transactions par Carte du Commerçant sont effectuées en utilisant une combinaison des options de sécurité améliorée suivantes :

- **La technologie EMV, EMV sans contact ou de Portefeuille numérique** – sur un appareil à puce actif possédant une homologation/certification EMVCo (www.emvco.com) valide et à jour et capable de traiter des Transactions par Carte à puce conformes AEIPS. (Les Commerçants des États-Unis doivent inclure le Sans-contact)
- **Le chiffrement de bout en bout (P2PE)** – communiqué au processeur du Commerçant à l'aide d'un système de chiffrement de bout en bout agréé par la norme PCI SSC ou un QSA
- **La tokénisation** – la solution mise en œuvre doit :
  - respecter les spécifications EMVCo,
  - être sécurisée, traitée, stockée, transmise et entièrement gérée par un prestataire de service tiers en conformité PCI, et
  - le Jeton (token) ne peut pas être décrypté pour révéler les Numéros de compte principal (PAN) non chiffrés au Commerçant.

Les Commerçants admissibles au Programme d'amélioration des technologies de la sécurité (STEP) ont des exigences relatives aux Documents de validation PCI réduites, comme il est décrit dans la Mesure 3 : « Réalisation des Documents de validation à envoyer à American Express » ci-dessous.

Mesure 3: Réalisation des Documents de validation à envoyer à American Express

Les documents suivants sont requis pour les différents niveaux de Commerçants et de Prestataires de services comme indiqué dans le Tableau A-2 : Documents de validation Commerçants et dans le Tableau A-3 : Documents de validation des Prestataires de services ci-dessus.

Vous devez fournir l'Attestation de conformité (Attestation of Compliance, AOC) pour le type d'évaluation applicable. L'AOC est une déclaration de votre état de conformité et, en tant que telle, doit être signée et datée par un responsable de niveau approprié au sein de votre organisation.

En plus de l'AOC, American Express peut vous demander de fournir une copie de l'évaluation complète et, à son entière discrétion, des documents justificatifs supplémentaires qui prouvent votre conformité avec les exigences de la norme PCI DSS. La réalisation de ces Documents de validation est entièrement à votre charge.

Rapport sur la conformité Attestation de conformité (ROC AOC) - (Obligation annuelle) – Le Rapport sur la conformité présente les résultats d'un examen détaillé sur site de vos équipements, systèmes et réseaux (et de leurs composants) dans lesquels les Données des Titulaires de Carte ou les Données d'authentification sensibles (ou les deux) sont enregistrées, traitées ou transmises. Il en existe deux versions : une pour les Commerçants et l'autre pour les Prestataires de services. Le Rapport sur la conformité doit être effectué par :

- un QSA, ou
- un Évaluateur de sécurité interne (ISA, Internal Security Assessor) avec attestation par votre directeur général, votre directeur financier, votre directeur de la sécurité des informations ou tout autre signataire autorisé de votre entreprise

Le ROC AOC doit être signé et daté par un QSA ou un ISA et un responsable de niveau autorisé au sein de votre organisation, puis transmis à American Express au minimum une fois par an.

Questionnaire d'autoévaluation Attestation de conformité (SAQ AOC) - (Obligation annuelle)– Les Questionnaires d'autoévaluation permettent de réaliser l'autoévaluation de vos équipements, systèmes et réseaux (et de leurs composants) dans lesquels les Données des Titulaires de Carte ou les Données d'authentification sensibles (ou les deux) sont enregistrées, traitées ou transmises. Il existe plusieurs versions du SAQ. Vous devrez en sélectionner au minimum un en fonction de votre Environnement de Données des Titulaires de Carte.

Le SAQ doit être réalisé par le personnel de votre Entreprise qui est qualifié pour répondre aux questions de manière précise et exhaustive ; vous pouvez également faire appel à un QSA pour vous aider. Le SAQ AOC doit être signé et daté par un responsable de niveau autorisé au sein de votre organisation, puis transmis à American Express au minimum une fois par an.

Résumé de l'examen des vulnérabilités externes du réseau réalisé par un Prestataire de services d'analyse agréé (Examen ASV) - (Tous les 90 jours) – L'examen de vulnérabilité externe est une procédure de test à distance qui vous permet d'identifier les faiblesses, les vulnérabilités et les erreurs de configuration potentielles des composants connectés à Internet de votre Environnement de Données des Titulaires de Carte (sites Web, applications, serveurs Web, serveurs de messagerie, domaines accessibles au public ou hôtes).

L'Examen ASV doit être réalisé par un Prestataire de services d'analyse agréé (Approved Scanning Vendor, ASV).

Si requis par le SAQ, l'Attestation d'analyse ASV de conformité de l'examen (Attestation of Scan Compliance, AOSC) ou le résumé, y compris le nombre de cibles examinées, la certification de la conformité des résultats aux procédures d'examen PCI DSS et l'état de conformité réalisé par l'ASV doivent être envoyés à American Express tous les 90 jours au minimum.

Si vous soumettez un ROC AOC ou STEP, vous n'êtes pas tenu de fournir une AOSC ou un résumé de l'Examen ASV, sauf dans le cas où cela vous a été spécifiquement demandé. Pour éviter toute ambiguïté, les Examens sont obligatoires si demandés par le Questionnaire d'autoévaluation (SAQ) applicable.

Documents de validation de l'Attestation du Programme STEP (STEP) - (Obligation annuelle) – STEP est uniquement disponible pour les Commerçants qui répondent aux critères indiqués à la Mesure 2 : « Compréhension de votre niveau Commerçant/de Prestataire de service et des exigences à respecter en matière de documents de validation » ci-dessus. Si votre entreprise remplit ces critères, vous devez remplir et envoyer le formulaire d'Attestation du Programme STEP chaque année à American Express. Le formulaire d'Attestation annuelle du Programme STEP peut être téléchargé via le Portail. Vous pouvez également prendre contact avec votre chargé de clientèle ou écrire à American Express à l'adresse AXPPCIComplianceProgram@aexp.com.

Non-conformité avec la norme PCI DSS - (Annuel, Tous les 90 jours et/ou Sur demande) – Si vous n'êtes pas en conformité avec la norme PCI DSS, vous devez envoyer un Résumé de l'outil d'approche par ordre de priorité PCI (disponible en téléchargement sur le site Web du PCI Security Standards Council).

Le résumé de l'outil d'approche par ordre de priorité doit désigner une date de résolution du problème ne dépassant pas douze (12) mois à compter de la date de finalisation du document afin d'assurer la conformité. Vous devez informer American Express régulièrement de votre progression dans la résolution des problèmes selon l'état de non-conformité (Commerçants de niveau 1, de niveau 2, de niveau 3 et de niveau 4 ; tous les Prestataires de services). La réalisation des mesures de résolution nécessaires pour assurer la conformité avec la norme PCI DSS est à votre charge.

American Express ne vous imposera pas de frais de non-conformité avant la date de résolution des problèmes. Conformément au Tableau A-4 : Frais de non-conformité, vous restez responsable à l'égard d'American Express de toutes les obligations d'indemnisation pour un Incident touchant les données et êtes soumis à toutes les autres dispositions de cette politique.

American Express se réserve le droit, à sa seule discrétion, d'imposer des frais de non-conformité si :

- un modèle d'approche par ordre de priorité PCI n'a pas été soumis conformément aux exigences stipulées dans cette section ;
- les étapes de résolution des problèmes décrites dans le modèle d'approche par ordre de priorité PCI pour l'état de non-conformité n'ont pas été respectées ;
- l'une des exigences du modèle d'approche par ordre de priorité PCI pour l'état de non-conformité n'a pas été remplie ; ou
- les documents de conformité obligatoires n'ont pas été fournis à American Express dans les délais impartis ou sur demande.

Les Commerçants/Prestataires de services qui ne respectent pas les exigences indiquées dans la Mesure 2: Compréhension de votre niveau Commerçant/de Prestataire de service et des exigences à respecter en matière de documents de validation, peuvent être soumis à des frais comme stipulé dans la Mesure 4: Envoi des Documents de validation à American Express.

Afin d'éviter toute confusion, les Commerçants qui ne sont pas conformes à la norme PCI DSS ne sont pas admissibles au Programme STEP.

Mesure 4: Envoi des Documents de validation à American Express

Tous les Commerçants et les Prestataires de services qui sont tenus de participer au Programme doivent envoyer les Documents de validation marqués « obligatoires » dans les tableaux de la Mesure 2 : « Compréhension de votre niveau Commerçant/de Prestataire de service et des exigences à respecter en matière de documents de validation » à American Express dans les délais impartis.

Vous devez envoyer vos Documents de validation à American Express via le Portail fourni par l'Administrateur du Programme sélectionné par American Express. Lorsque vous envoyez les Documents de validation, vous déclarez et garantissez à American Express que les déclarations suivantes sont véridiques (pour autant que vous le sachiez) :

- Votre évaluation est complète et exhaustive ;
- L'état PCI DSS est fidèlement représenté au moment de son évaluation, qu'il s'agisse de la soumission de l'Attestation de conformité (AOC) ou d'un Résumé de l'outil d'approche par ordre de priorité (PAT) pour non-conformité ;
- Vous êtes autorisé à divulguer les informations qui y sont contenues et vous fournissez les Documents de validation à American Express sans violer les droits d'aucune autre partie.

Frais de non-conformité et résiliation du Contrat

American Express a le droit de vous imposer des frais de non-conformité et de résilier le Contrat si vous ne répondez pas à ces exigences ou si vous ne fournissez pas les Documents de validation obligatoires à American Express dans le délai imparti. American Express tentera d'informer la personne à contacter pour les questions de sécurité de la date limite fixée pour chaque période de rapport annuelle et trimestrielle.

Tableau A-4 : Frais de non-conformité

Description*	Commerçant ou Prestataire de services de niveau 1	Commerçant ou Prestataire de services de niveau 2	Commerçant de niveau 3 ou de niveau 4
Des frais de non-conformité seront appliqués si les documents de validation ne sont pas reçus avant la première échéance.	25 000 $ USD	5 000 $ USD	50 $ USD
Des frais de non-conformité supplémentaires seront appliqués si les documents de validation ne sont pas reçus avant la deuxième échéance.	35 000 $ USD	10 000 $ USD	100 $ USD
Des frais de non-conformité supplémentaires seront appliqués si les documents de validation ne sont pas reçus avant la troisième échéance. **REMARQUE :** L'application des frais de non-conformité sera renouvelée tant que les Documents de conformité ne sont pas envoyés.	45 000 $ USD	15 000 $ USD	250 $ USD

* Les frais de non-conformité seront appliqués selon l'équivalent en Devise locale.

* Non applicable en Argentine.

Si vous ne respectez pas vos obligations en matière de Documents de conformité PCI DSS, American Express aura le droit d'imposer de manière cumulative des frais pour non-conformité, de refuser des paiements et/ou de mettre fin au Contrat.

Section 3 Obligations concernant la gestion des Incidents touchant les données

Vous devez avertir American Express immédiatement et en aucun cas au-delà de soixante-douze (72) heures après la découverte d'un Incident touchant les données.

Pour avertir American Express, veuillez contacter le programme d'intervention de l'entreprise American Express en cas d'incident (*EIRP*) gratuitement au +1.888.732.3750 ou au +1.602.537.3021 , ou par courrier électronique à EIRP@aexp.com. Vous devez désigner la personne à contacter concernant ces Incidents touchant les données. En outre :

- Vous devez mener une enquête approfondie pour chaque Incident touchant les données et vous devez immédiatement fournir à American Express tous les Numéros de Carte compromis. American Express se réserve le droit d'effectuer sa propre analyse interne pour identifier les données impliquées dans l'Incident touchant les données.

Pour les Incidents touchant les données impliquant moins de 10 000 Numéros de Carte uniques, un résumé d'enquête doit être fourni à American Express sous dix (10) jours ouvrables après sa finalisation.

- Les résumés d'enquête doivent contenir les informations suivantes : Résumé de l'incident, description du ou des environnements concernés, chronologie des événements, dates clés, détails concernant l'impact et l'exposition des données, mesures prises pour endiguer et résoudre l'incident, et attestation selon laquelle rien n'indique que d'autres données d'American Express sont à risque.

Pour les Incidents impliquant 10 000 Numéros de Carte uniques ou plus, vous devez engager un Enquêteur judiciaire PCI (PFI) pour mener cette enquête sous cinq (5) jours à compter de la découverte d'un Incident touchant les données.

- Le rapport d'enquête non modifié doit être fourni à American Express, sous dix (10) jours ouvrés après sa finalisation.
- Les rapports d'enquête judiciaire doivent être réalisés à l'aide du Modèle de rapport final d'incident légal disponible par le biais de la PCI. Ce rapport doit inclure des examens et des rapports judiciaires concernant la conformité et toutes les informations relatives à l'Incident, identifier la cause de l'Incident, confirmer si vous étiez ou non en conformité avec la norme PCI DSS au moment de l'Incident et vérifier votre aptitude à éviter de futurs Incidents touchant des données en (i) fournissant un plan visant à remédier à tous les manquements à la norme PCI DSS, et (ii) en participant au programme de conformité d'American Express (comme décrit ci-dessous). À la demande d'American Express, vous devrez faire valider la résolution des problèmes par un Évaluateur qualifié en matière de sécurité (Qualified Security Assessor, QSA).

Nonobstant les paragraphes précédents de la Section 3, « Obligations concernant la gestion des Incidents touchant les données » :

- American Express pourra, à son entière discrétion, demander que vous engagiez un PFI pour mener l'enquête sur un Incident touchant les données impliquant moins de 10 000 Numéros de Carte uniques ou lorsque plusieurs incidents se sont produits au cours d'une période de 12 mois. Toute enquête de ce type doit être conforme aux exigences énoncées plus haut à la Section 3, « Obligations concernant la gestion des Incidents touchant les données », et finalisée dans les délais requis par American Express.
- American Express pourra, à son entière discrétion, engager séparément un PFI pour mener l'enquête sur tout Incident touchant les données et vous imputer le coût de ladite enquête.

Vous devez évaluer l'Incident touchant les données au regard des lois applicables sur la notification des violations de données à l'échelle mondiale et, lorsque cela s'avère nécessaire, avertir les organismes de contrôle et les Titulaires de la Carte concernés conformément à ces lois sur la notification des violations de données. Si vous avez déterminé qu'il incombe à votre Prestataire de services ou à une autre entité de signaler l'Incident touchant les données, vous devez informer ce Prestataire de services ou cette entité de son devoir d'évaluer ses obligations de signalement en vertu des lois applicables sur la notification des violations de données. Vous acceptez d'obtenir l'accord écrit d'American Express avant de mentionner ou de nommer American Express dans toute communication adressée à des Titulaires de la Carte concernant l'Incident touchant les données. Vous acceptez de collaborer avec American Express afin de fournir des détails et de rectifier tout problème résultant de l'Incident touchant les données, notamment en fournissant à American Express toutes les informations nécessaires (et en obtenant toute dérogation nécessaire pour les fournir) afin de vérifier votre aptitude à éviter de futurs Incidents touchant les données, conformément au Contrat.

Nonobstant toute obligation de confidentialité contraire au Contrat, American Express a le droit de divulguer des informations concernant tout Incident aux Titulaires de Carte American Express, aux émetteurs, aux autres participants du réseau American Express et au grand public conformément à la Loi en vigueur ; par une décision judiciaire, administrative ou réglementaire, un décret, une citation à comparaître, une demande ou toute autre procédure en vue de réduire le risque de fraude, d'autres risques ou autre, dans une mesure appropriée à l'exploitation du réseau American Express.

Que faire en cas d'Incident touchant les données ?

Veuillez suivre les étapes suivantes lorsque vous avez identifié un Incident touchant les données dans votre entreprise.

Étape 1 :

Remplir le Formulaire Commerçant de signalement initial d'un Incident touchant les données et l'envoyer par courrier électronique à EIRP@aexp.com dans les 72 heures après la découverte d'un Incident touchant les données.

Étape 2 :

Mener une enquête approfondie ; cela peut nécessiter de faire appel à un Enquêteur judiciaire PCI (Payment Card Industry).

Étape 3 :

Immédiatement nous fournir tous les Numéros de Carte American Express® compromis.

Étape 4 :

Collaborer avec nous afin de résoudre tout problème résultant de l'Incident touchant les données.

Consulter la Section 3, « Obligations concernant la gestion des Incidents touchant les données » pour de plus amples informations sur les Obligations concernant la gestion des Incidents touchant les données.

Des questions ?

États-Unis : (888) 732-3750 (gratuit)

International : +1 (602) 537-3021

EIRP@aexp.com

Section 4 Obligations en matière d'indemnisation en cas d'Incident touchant les données

Vos obligations d'indemnisation envers American Express en vertu du Contrat concernant les Incidents touchant les données sont déterminées dans la Section 4, « Obligations en matière d'indemnisation en cas d'Incident touchant les données », sans annuler les autres droits et recours d'American Express. Outre vos obligations en matière d'indemnisation (le cas échéant), vous pourrez être sujet à des frais de non-conformité pour un Incident touchant les données comme décrit ci-dessous, dans la Section 4, « Obligations en matière d'indemnisation en cas d'Incident touchant les données ».

Vous devrez dédommager American Express à raison de 5 USD par numéro de compte, pour les Incidents touchant les données qui impliquent :

- 10 000 Numéros de Carte American Express ou plus et l'un des éléments suivants :
  - Données d'authentification sensibles, ou
  - Date d'expiration

Toutefois, American Express ne vous demandera pas d'indemnisation pour un Incident touchant les données impliquant :

- moins de 10 000 Numéros de Carte American Express, ou
- plus de 10 000 Numéros de Carte American Express, si vous remplissez les conditions suivantes :
  - vous avez informé American Express à propos de l'Incident en vertu de la Section 3, « Obligations concernant la gestion des Incidents touchant les données »,

- vous étiez en conformité au moment de l'Incident avec la norme PCI DSS (déterminée par l'enquête du PFI sur l'Incident), et
- l'Incident n'a pas été causé par un comportement fautif de votre part ou de la part de vos Parties assujetties.

Nonobstant les paragraphes précédents de la Section 4, « Obligations en matière d'indemnisation en cas d'Incident touchant les données », pour tout Incident touchant les données, quel que soit le nombre de Numéros de Carte American Express, vous devrez payer à American Express des frais de non-conformité pour l'Incident, qui ne dépasseront pas 100 000 USD par Incident (comme déterminé par American Express à sa seule discrétion) en cas de manquement à l'une de vos obligations énoncées dans la Section 3, « Obligations concernant la gestion des Incidents touchant les données ». Pour éviter toute ambiguïté, le total des frais de non-conformité pour un Incident touchant les données ne devra pas dépasser 100 000 USD par Incident.

Pour le calcul, American Express ne tiendra pas compte de tout numéro de compte-Carte American Express impliqué dans une demande d'indemnisation précédente pour Incident touchant les données faite dans les douze (12) mois qui précèdent la Date de signalement. Tous les calculs effectués par American Express conformément à cette méthode sont définitifs.

American Express pourra vous facturer le montant total de vos obligations d'indemnisation pour des Incidents touchant les données ou déduire le montant de paiements American Express à votre ordre (ou débiter votre Compte bancaire en conséquence) en vertu du Contrat.

Vos obligations d'indemnisation pour les Incidents touchant les données en vertu des présentes ne doivent pas être considérées comme des dommages-intérêts accessoires, indirects, spéculatifs, consécutifs, particuliers, punitifs ou exemplaires en vertu du Contrat ; à condition que ces obligations ne comprennent pas de dommages-intérêts liés à (ou de l'ordre de) la perte de profits ou de revenus, la perte de clientèle ou la perte d'opportunités commerciales.

À sa seule discrétion, American Express peut réduire l'obligation d'indemnisation pour les Commerçants uniquement en cas d'Incidents touchant les données répondant à tous les critères suivants :

- les Technologies d'atténuation des risques applicables ont été utilisées avant l'Incident touchant les données et étaient utilisées durant toute la Période d'événement de l'Incident touchant les données ;
- Une enquête approfondie conformément au programme PFI a été effectuée (sauf accord contraire par écrit auparavant) ;
- le rapport légal indique clairement les Technologies d'atténuation des risques applicables qui ont été utilisées pour traiter, stocker et/ou transmettre les données au moment de l'Incident touchant les données ; et
- vous ne stockez pas (et vous n'avez pas stocké durant la Période d'événement de l'Incident touchant les données) des Données d'authentification sensibles ni d'autres Données de Titulaires de Carte qui n'ont pas été rendus illisibles.

Lorsqu'une réduction de l'indemnisation est disponible, la réduction appliquée à votre obligation d'indemnisation (à l'exception des frais pour non-conformité dus), est déterminée comme suit :

Tableau A-5 : Critères requis pour la réduction de l'obligation d'indemnisation

Réduction de l'obligation d'indemnisation	Critères requis
Réduction standard : 50 %	> 75 % du total des Transactions traitées sur des appareils acceptant les Cartes à puce[1] OU
	Technologie d'atténuation des risques utilisée dans > 75 % des Établissements du Commerçant[2]
Réduction renforcée : 75 % à 100 %	> 75 % de toutes les Transactions traitées sur des appareils acceptant les Cartes à puce[1] ET une autre Technologie d'atténuation des risques utilisée dans > 75 % des Établissements du Commerçant[2]

[1] Déterminé par l'analyse interne d'American Express

[2] Déterminé par l'enquête PFI

- La Réduction renforcée (75 à 100 %) doit être déterminée sur la base du pourcentage le moins élevé de Transactions utilisant des appareils acceptant les Cartes à puce ET d'Établissements utilisant une autre Technologie d'atténuation des risques. Les exemples présentés dans le Tableau A-6 : Réduction renforcée de l'obligation d'indemnisation illustrent le calcul de la réduction de l'indemnisation.
- Pour remplir les critères d'utilisation de Technologie d'atténuation des risques, vous devez prouver que vous utilisez effectivement la technologie conformément à sa conception et à ses objectifs prévus.
- Le pourcentage de vos établissements qui utilisent une Technologie d'atténuation des risques est déterminé par l'enquête PFI.
- La réduction de l'obligation d'indemnisation ne s'applique pas aux frais pour non-conformité dus concernant l'Incident touchant les données.

Tableau A-6 : Réduction renforcée de l'obligation d'indemnisation

Ex.	Technologies d'atténuation des risques utilisées	Admissible	Réduction
1	• 80 % des Transactions sur des appareils acceptant les Cartes à puce • 0 % des Établissements utilisent une autre Technologie d'atténuation des risques	Non	50 % : Réduction standard (une utilisation inférieure à 75 % d'une Technologie d'atténuation des risques ne remplit pas les critères pour être admissible à une réduction renforcée)[1]
2	• 80 % des Transactions sur des appareils acceptant les Cartes à puce • 77 % des Établissements utilisent une autre Technologie d'atténuation des risques	Oui	77 % : Réduction renforcée (sur la base d'une utilisation de 77 % d'une Technologie d'atténuation des risques)
3	• 93 % des Transactions sur des appareils acceptant les Cartes à puce • 100 % des Établissements utilisent une autre Technologie d'atténuation des risques	Oui	93 % : Réduction renforcée (sur la base de 93 % des Transactions sur des appareils acceptant les Cartes à puce)
4	• 40 % des Transactions sur des appareils acceptant les Cartes à puce • 90 % des Établissements utilisent une autre Technologie d'atténuation des risques	Non	50 % : Réduction standard (si moins de 75 % des Transactions sont effectuées sur des appareils acceptant les Cartes à puce, vous ne remplissez pas les critères pour être admissible à une réduction renforcée)

[1] Un Incident touchant les données concernant 10 000 comptes de Carte American Express, au taux de 5 USD par numéro de compte (10 000 x 5 USD = 50 000 USD) peut être admissible à une réduction de 50 %, ce qui diminue les obligations d'indemnisation de 50 000 USD à 25 000 USD, à l'exception des frais pour non-conformité éventuels.

Section 5 Programme d'analyse ciblée (Targeted Analysis Programme, TAP)

Les mises en danger de Données de Titulaires de Carte peuvent provenir de failles de sécurité des données dans votre Environnement de Données des Titulaires de Carte (Cardholder Data Environment, CDE).

Comme exemples de mise en danger potentielle de Données de Titulaires de Carte, citons notamment :

- **Point de vente commun (Common Point of Purchase, CPP) :** Des Titulaires de la Carte American Express signalent des Transactions frauduleuses sur leurs comptes-Cartes pour lesquelles vos Établissements sont identifiés comme le point d'origine des achats.
- **Données de Carte Retrouvées :** Des Données de Carte American Express et de Titulaire de Carte retrouvées sur le Web sont associées à des Transactions effectuées dans vos Établissements.
- **Logiciel malveillant soupçonné :** American Express soupçonne que vous utilisez un logiciel qui est infecté par un code malveillant ou qui y est vulnérable.

Le TAP vise à identifier les mises en danger potentielles de Données de Titulaires de Carte.

Vous, ainsi que vos Parties assujetties, devez respecter les exigences suivantes dès la notification, transmise par American Express, d'une mise en danger potentielle de Données de Titulaires de Carte.

- Vous devez immédiatement inspecter votre CDE afin d'identifier les failles de sécurité des données et y remédier.
  - Vous devez demander à vos prestataires tiers d'inspecter minutieusement votre CDE si externalisé.
- Vous devez fournir un récapitulatif des mesures prises ou planifiées à la suite de votre inspection, évaluation et/ou de vos efforts de résolution dès que vous recevez la notification d'American Express.
- Vous devez fournir des documents à jour de validation de la norme PCI DSS conformément à la Section 2, « Programme de conformité à la norme PCI DSS (Validation périodique importante de vos systèmes) ».
- Le cas échéant, vous devez engager un Enquêteur judiciaire PCI PFI agréé afin d'inspecter votre CDE si vous, ou vos Parties assujetties :
  - Ne pouvez pas résoudre la mise en danger de Données de Titulaires de Carte dans un délai raisonnable, tel que déterminé par American Express, ou
  - Confirmez qu'un Incident touchant les données s'est produit et respectez les exigences stipulées dans la Section 3, « Obligations concernant la gestion des Incidents touchant les données ».

Tableau A-7 : Frais pour non-conformité au TAP

Description	Commerçant ou Prestataire de services de niveau 1	Commerçant ou Prestataire de services de niveau 2	Commerçant de niveau 3 ou de niveau 4
Des frais de non-conformité peuvent être appliqués en cas de non-respect des obligations du TAP avant la première échéance.	25 000 $ USD	5 000 $ USD	1 000 $ USD
Des frais de non-conformité peuvent être appliqués en cas de non-respect des obligations du TAP avant la deuxième échéance.	35 000 $ USD	10 000 $ USD	2 500 $ USD
Des frais de non-conformité peuvent être appliqués en cas de non-respect des obligations du TAP avant la troisième échéance. **REMARQUE :** *L'application des frais de non-conformité peut être renouvelée tant que les obligations ne sont pas respectées ou le TAP n'est pas résolu.*	45 000 $ USD	15 000 $ USD	5 000 $ USD

Si vous ne respectez pas les obligations du TAP, American Express aura le droit d'imposer de manière cumulative des frais pour non-conformité, de refuser des paiements et/ou de mettre fin au Contrat.

Section 6 Confidentialité

American Express prendra des mesures raisonnables pour garantir la confidentialité (et s'assurera que ses agents et sous-traitants, y compris le fournisseur du Portail, garantissent la confidentialité) de vos rapports sur la conformité, y compris la documentation de validation et pour ne pas divulguer la documentation de validation à des tiers (autres que les Filiales, agents, représentants, Prestataires de services et sous-traitants d'American Express) pour une période de trois ans à compter de la date de réception. Cette obligation de confidentialité ne s'applique pas à la documentation de validation qui :

a. a déjà été portée à la connaissance d'American Express avant la divulgation ;

b. est ou devient disponible au public sans violation du présent paragraphe par American Express ;

c. est légitimement envoyée à American Express par un tiers sans obligation de confidentialité ;

d. est créée indépendamment par American Express ; ou

e. doit être divulguée sur ordre d'un tribunal, d'un organisme administratif ou d'une autorité gouvernementale, ou par une loi, une règle ou une réglementation, par une citation à comparaître, une demande de remise de document, une assignation ou toute autre procédure judiciaire ou administrative ou par toute enquête officielle ou non d'une autorité ou agence gouvernementale (notamment les régulateurs, inspecteurs, examinateurs ou organismes chargés de l'application de la loi).

Section 7 Clause de non-responsabilité

PAR LA PRÉSENTE, AMERICAN EXPRESS DÉCLINE TOUTE REPRÉSENTATION, GARANTIE ET RESPONSABILITÉ PAR RAPPORT À CETTE POLITIQUE OPÉRATIONNELLE DE SÉCURITÉ DES DONNÉES, LA NORME PCI DSS, LES SPÉCIFICATIONS EMV ET LA DÉSIGNATION ET LES PERFORMANCES DES QSA, ASV OU PFI (OU DES TROIS), QUE CELLES-CI SOIENT EXPLICITES, IMPLICITES, STATUTAIRES OU AUTRES, Y COMPRIS TOUTE GARANTIE DE QUALITÉ MARCHANDE OU D'ADAPTATION À UN USAGE PARTICULIER. LES ÉMETTEURS DE CARTES AMERICAN EXPRESS NE SONT PAS DES TIERS BÉNÉFICIAIRES SELON CETTE POLITIQUE.

Section 8 Glossaire

Les définitions suivantes s'appliquent uniquement pour les besoins de la présente *Politique de sécurité des données*, et elles auront préséance en cas de conflit avec les conditions qui se trouvent dans le *Règlement Commerçant*.

Appareil à puce désigne un appareil de point de vente possédant une homologation/certification EMVCo (www.emvco.com) valide et à jour et capable de traiter des Transactions par Carte à puce compatibles avec AEIPS.

Application de paiement a le sens qui lui est donné dans le glossaire des termes alors en vigueur pour les normes Secure Software Standard (norme de sécurité des logiciels) et Secure Software Life Cycle Standard (norme de sécurité du cycle de vie des logiciels), disponible sur www.pcisecuritystandards.org.

Approuvé par la PCI signifie qu'un Dispositif de saisie du code PIN ou une application de paiement (ou les deux) apparaît au moment du déploiement sur la liste des entreprises et fournisseurs agréés établie par le PCI Security Standards Council, SARL, disponible sur www.pcisecuritystandards.org.

Attestation de conformité (AOC) désigne une déclaration de l'état de votre conformité avec la norme PCI DSS, dans le formulaire fourni par le Payment Card Industry Security Standards Council, SARL.

Attestation de conformité de l'examen (AOSC) désigne une déclaration de l'état de votre conformité avec la norme PCI DSS basée sur un examen de réseau, dans le formulaire fourni par le Payment Card Industry Security Standards Council, SARL.

Carte à puce désigne une carte qui contient une puce et peut nécessiter un code PIN afin de vérifier l'identité du Titulaire de Carte ou les données du compte contenues sur la puce, ou les deux (parfois appelée « carte intelligente », « Carte EMV », « ICC » ou « carte à circuit intégré » dans nos documents).

Carte American Express ou **Carte** désigne toute carte, tout dispositif d'accès aux comptes ou dispositif ou service de paiement portant le nom, le logo, la marque de commerce, la marque de service, le nom commercial d'American Express ou d'une Filiale, ou toute conception ou désignation exclusive et émis par un émetteur ou un numéro de compte-Carte.

Chiffrement bout en bout (P2PE) désigne une solution qui protège de manière cryptographique les données de compte, du point où un commerçant accepte la carte de paiement au point sécurisé de déchiffrement.

Clé de cryptage (« Clé de cryptage American Express ») désigne toutes les Clés utilisées dans le traitement, la création, le chargement et/ou la protection de données de comptes. Cela concerne, sans toutefois s'y limiter :

- principales Clés de cryptage : Clés maîtresses de zones (ZMK) et Clés de codes PIN de zones (ZPK) ;
- Clés maîtresses utilisées dans les dispositifs cryptographiques sécurisés : Clés maîtresses locales (LMK) ;
- Clés des codes de sécurité des Cartes (CSCK) ;
- Clés PIN : Clés de dérivation de base (BDK), Clés de cryptage de codes PIN (PEK) et ZPK.

Commerçant désigne le Commerçant et toutes ses Filiales qui acceptent les Cartes American Express dans le cadre d'un Contrat avec American Express ou ses Filiales.

Commerçant de niveau 1 désigne un Commerçant réalisant 2,5 millions de Transactions de Cartes American Express ou plus par an ; ou tout commerçant qu'American Express estime être de niveau 1.

Commerçant de niveau 2 désigne un Commerçant réalisant de 50 000 à moins de 2,5 millions de Transactions de Cartes American Express par an.

Commerçant de niveau 3 désigne un Commerçant réalisant de 10 000 à moins de 50 000 Transactions de Cartes American Express par an.

Commerçant de niveau 4 désigne un Commerçant réalisant moins de 10 000 Transactions de Cartes American Express par an.

Consommateur désigne un titulaire de la carte qui achète des biens, des services, ou les deux.

Contrat désigne les Conditions générales, le Règlement Commerçant, et les annexes et pièces connexes, collectivement (parfois désigné sous le nom de Contrat d'acceptation de la Carte dans notre documentation).

Crédit désigne le montant de l'opération que vous remboursez aux Titulaires de Carte pour les achats ou les paiements effectués avec la Carte.

Date de signalement désigne la date à laquelle American Express envoie aux émetteurs la notification finale d'Incident touchant les données. Cette date dépend de la date à laquelle American Express reçoit le rapport légal final ou l'analyse interne et doit être fixée à la seule discrétion d'American Express.

Débit désigne un paiement ou un achat effectué avec une Carte.

Dispositifs de saisie du code PIN a le sens qui lui est donné dans le glossaire des termes alors en vigueur pour les exigences en matière de sécurité modulaire et le point d'interaction (POI) pour la sécurité des Transactions par code PIN (PTS) de l'industrie des Cartes de paiement, disponible sur www.pcisecuritystandards.org.

Documents de validation désigne l'AOC rendue avec une évaluation annuelle de sécurité sur site ou SAQ, l'AOSC et les résumés des résultats rendus avec les examens trimestriels du réseau ou l'Attestation annuelle du Programme d'amélioration des technologies de la sécurité.

Données d'authentification sensibles désigne les informations liées à la sécurité, utilisées pour authentifier les titulaires de la carte et/ou autoriser les transactions par carte de paiement. Ces informations incluent, sans toutefois s'y limiter, les codes de vérification de la carte, les données complètes (de la bande magnétique ou de l'équivalent sur une carte à puce), les codes PIN et les blocs PIN.

Données de compte se composent des Données des Titulaires de Carte et/ou des Données d'authentification sensibles. Se reporter aux entrées Données du Titulaire de la Carte et Données d'authentification sensibles.

Données de Transaction désigne toutes les informations exigées par American Express, attestant une ou plusieurs Transactions, y compris les informations obtenues au point de vente, les informations obtenues ou générées au cours de l'Autorisation et de la Soumission, et les éventuelles Actions Compensatoires.

Données des Titulaires de la Carte signifie, au minimum, le numéro de compte principal (PAN) complet utilisé seul ou le PAN complet accompagné des informations suivantes : nom du titulaire de la carte, date d'expiration et/ou code de service. Se reporter à l'entrée Données d'authentification sensibles pour connaitre les éléments de données supplémentaires qui peuvent être transmis ou traités (mais non stockés) dans le cadre d'une transaction de paiement.

Émetteur de Carte désigne toute Entité (y compris American Express et ses Affiliés) qui est habilitée par American Express ou un Affilié d'American Express à émettre des Cartes et à mener des activités d'émission de Carte.

Enregistrement de Crédit désigne un Enregistrement de Crédit conforme à nos exigences.

Enregistrement de Débit désigne un enregistrement reproductible (à la fois sur support papier et électronique) d'un Débit conforme à nos exigences et qui contient le numéro de la Carte, la date de la Transaction, le montant en dollars, l'Approbation, la signature du Titulaire de la Carte (le cas échéant), et d'autres informations.

Enquêteur judiciaire PCI (PFI) désigne une entité qui a été approuvée par le Payment Card Industry Security Standards Council, SARL pour effectuer des enquêtes judiciaires sur des violations ou mises en danger de données de Cartes de paiement.

Environnement de Données des Titulaires de Carte (CDE) désigne les personnes, les processus et les technologies qui stockent, traitent ou transmettent les données des titulaires de cartes ou les données d'authentification sensibles.

Évaluateur qualifié en matière de sécurité (QSA) désigne une entité qualifiée par le Payment Card Industry Security Standards Council, SARL pour valider le respect de la norme PCI DSS.

Exigences en matière de sécurité des codes PIN PCI désigne les Exigences en matière de sécurité des codes PIN de l'industrie des Cartes de paiement, disponibles sur www.pcisecuritystandards.org.

Exigences Payment Card Industry Security Standards Council (PCI SSC) désigne les normes et exigences en matière de sécurité et de protection des données de cartes de paiement, y compris celles du PCI DSS et PA DSS, disponibles sur www.pcisecuritystandards.org.

Franchisé désigne un tiers détenu et fonctionnant de manière indépendante (franchisé, sous licence ou branche), autre qu'un Affilié, qui est habilité par un Franchiseur pour exploiter une franchise et qui a signé un contrat écrit avec le Franchiseur selon lequel il affiche uniformément et de manière évidente son identification munie des Marques du Franchiseur ou se présente au public comme faisant partie du groupe de sociétés du Franchiseur.

Franchiseur désigne l'exploitant d'une entreprise qui habilite des personnes ou entités (Franchisés) à distribuer des produits et/ou des services sous la marque de l'opérateur, ou à exercer des activités en utilisant celle-ci ; fournit une assistance aux Franchisés pour exploiter leur entreprise ou influence le mode de fonctionnement des Franchisés ; et exige le paiement de frais par les Franchisés.

Incident touchant les données désigne un incident impliquant la mise en danger ou la mise en danger soupçonnée de Clés de cryptage American Express ou au moins un numéro de compte-Carte American Express pour lequel il y a :

- une utilisation ou un accès non autorisé aux Clés de cryptage, aux Données des Titulaires de Carte ou aux Données d'authentification sensibles (ou une combinaison de celles-ci) qui sont enregistrées, traitées ou transmises sur vos équipements, systèmes et/ou réseaux (ou leurs composants) ou dont vous demandez, fournissez ou mettez à disposition l'utilisation ;
- une utilisation de ces Clés de cryptage, Données des Titulaires de Carte ou Données d'authentification sensibles (ou une combinaison de celles-ci) autre que celle prévue par le Contrat ; et/ou
- la perte, le vol ou le détournement présumé ou confirmé par tout moyen de tout support, document, enregistrement ou de toutes informations contenant ces Clés de cryptage, Données des Titulaires de Carte ou Données d'authentification sensibles (ou une combinaison de celles-ci).

Informations sur le Titulaire désigne les données concernant les Titulaires de Carte et les Transactions de Cartes American Express, y compris les noms, adresses, numéros de compte-Carte et numéros d'identification de Cartes (CID).

Jeton désigne le jeton cryptographique qui remplace le PAN, en fonction d'un indice donné pour une valeur non prévisible.

Modèle de rapport final d'incident légal désigne le modèle publié par le PCI Security Standards Council, disponible sur le site www.pcisecuritystandards.org.

Niveau Commerçant signifie la désignation que nous attribuons aux Commerçants qui détermine leurs obligations en matière de validation de la conformité à la norme PCI DSS, comme décrit dans la Section 2, « Programme de conformité à la norme PCI DSS (Validation périodique importante de vos systèmes) ».

Numéro de Carte compromis désigne un numéro de compte-Carte American Express lié à un Incident touchant les données.

Numéro de Carte désigne le numéro d'identification unique que l'Émetteur assigne à la Carte à son émission.

Numéro de compte principal (PAN) a le sens qui lui est donné dans le glossaire des termes alors en vigueur pour la norme PCI DSS.

Parties assujetties désigne tous vos employés, agents, représentants, sous-traitants, Processeurs, Prestataires de services, fournisseurs des équipements de point de vente (POS) ou systèmes ou solutions de traitement des paiements, Entités associées à votre Compte Commerçant American Express, et toute autre partie à laquelle vous pouvez accorder un accès aux Données du Titulaire de Carte ou aux Données d'authentification sensibles (ou les deux) conformément au Contrat.

Payment Card Industry Data Security Standard (PCI DSS) signifie une Norme de sécurité des données de l'industrie des Cartes de paiement, disponible sur www.pcisecuritystandards.org.

PCI DSS signifie une Norme de sécurité des données de l'industrie des Cartes de paiement, disponible sur www.pcisecuritystandards.org.

Période d'événement de l'incident touchant les données désigne la durée de l'intrusion (ou une période définie de manière similaire) indiquée dans le rapport d'enquête final (par ex., le rapport de l'Enquêteur judiciaire PCI), ou si elle n'est pas connue, les 365 jours maximum précédant la dernière Date de signalement des Numéros de Cartes potentiellement compromis, impliqués dans une mise en danger des Données qui nous a été signalée.

(Le) Portail désigne le système de transmission des rapports fourni par l'Administrateur du Programme PCI d'American Express sélectionné par American Express. Les Commerçants et Prestataires de services sont tenus d'utiliser le Portail pour envoyer les Documents de validation PCI à American Express.

Prestataire de services de niveau 1 désigne un Prestataire de services réalisant 2,5 millions de Transactions de Cartes American Express ou plus par an ; ou tout Prestataire de services qu'American Express estime être de niveau 1.

Prestataire de services de niveau 2 désigne un Prestataire de services réalisant moins de 2,5 millions de Transactions de Cartes American Express par an ; ou tout Prestataire de services qu'American Express n'estime pas être de niveau 1.

Prestataire de services d'analyse agréé (ASV) désigne une Personne morale qualifiée par le Payment Card Industry Security Standards Council, SARL pour valider le respect de certaines exigences de la norme PCI DSS en effectuant des examens de vulnérabilité d'environnements confrontés à Internet.

Prestataires de services désigne les processeurs, processeurs tiers, fournisseurs de passerelles, intégrateurs de Systèmes de point de vente, et les autres fournisseurs aux Commerçants de Systèmes de point de vente ou services de traitement des paiements pour les Commerçants.

Processeur désigne un prestataire de services aux Commerçants qui facilite le traitement des autorisations et soumissions du réseau American Express.

(Le) Programme désigne le Programme de conformité PCI d'American Express.

Programme d'amélioration des technologies de la sécurité (STEP) désigne le programme d'American Express dans lequel les Commerçants sont encouragés à déployer des technologies qui améliorent la sécurité des données.

Programme d'analyse ciblée désigne un programme qui fournit une détection précoce des mises en danger potentielles de données de Titulaires de Carte dans votre Environnement de Données des Titulaires de Carte (CDE). Se reporter à la Section 5, « Programme d'analyse ciblée (Targeted Analysis Programme, TAP) ».

Puce désigne une micropuce intégrée à une Carte contenant les données du Titulaire de Carte et du compte.

Questionnaire d'autoévaluation (SAQ) désigne un outil d'autoévaluation créé par le Payment Card Industry Security Standards Council, SARL, destiné à évaluer et attester du respect de la norme PCI DSS.

Solution de chiffrement de bout en bout (P2PE) agréée, figurant sur la liste des solutions validées par le PCI SSC ou par une entreprise P2PE Évaluateur qualifié en matière de sécurité PCI SSC (QSA).

Spécifications EMV désigne les spécifications émises par EMVCo, SARL, disponibles sur www.emvco.com.

Système de point de vente (POS) désigne un système ou équipement de traitement des données, y compris un terminal, un ordinateur personnel, une caisse enregistreuse électronique, un lecteur sans contact ou un outil ou processus de paiement, utilisé par un Commerçant pour obtenir des autorisations ou pour recueillir des données de Transactions, ou les deux.

Technologie d'atténuation des risques désigne des solutions technologiques qui améliorent la sécurité des Données et des Données d'authentification sensibles des Titulaires de Carte, déterminées par American Express. Pour remplir les critères de Technologie d'atténuation des risques, vous devez prouver que vous utilisez effectivement la technologie conformément à sa conception et à ses objectifs prévus. Les exemples comprennent, sans s'y limiter : la technologie EMV, le Chiffrement de bout en bout et la tokénisation.

Titulaire de Carte désigne une personne physique ou morale (i) qui a conclu un accord établissant un compte-Carte avec un émetteur ou (ii) dont le nom apparaît sur la Carte.

Titulaire de la Carte désigne un client auquel une carte de paiement est délivrée, ou toute personne autorisée à utiliser la carte de paiement.

Transaction désigne un Débit, un Crédit, une Avance de fonds (ou tout autre accès à des liquidités) ou une Transaction à un distributeur automatique effectuée au moyen d'une Carte.

Transaction émise par l'entreprise (BIP) désigne une solution de paiement numérique qui permet aux acheteurs de planifier rapidement et efficacement les paiements à l'intention des fournisseurs (en lien avec les cartes d'entreprise).

Transaction EMV désigne une Transaction par carte à circuit intégré (parfois appelée « Carte IC », « Carte à puce », « carte intelligente », « Carte EMV » ou « ICC ») effectuée sur un terminal de point de vente (POS) compatible avec les Cartes IC avec une approbation de type EMV valide et à jour. Les approbations de type EMV sont disponibles sur www.emvco.com.

Section 9 Sites Web utiles

Sécurité des données d'American Express : www.americanexpress.com/datasecurity

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

EMVCo: www.emvco.com