AMERICAN EXPRESS

Lignes directrices opérationnelles sur la sécurité des données (DSOP)

Icônes de changement

Les mises à jour importantes sont répertoriées dans le Tableau de synthèse des modifications et sont également indiquées dans la rubrique *DSOP* avec une icône de changement. Une icône de changement à côté du titre d'une section ou d'une sous-section indique que le texte de la section ou de la sous-section a été révisé, ajouté ou supprimé. Les changements dans le *DSOP* sont indiqués par une icône de changement comme celle-ci :

Tableau de synthèse des modifications

Les mises à jour importantes sont répertoriées dans le tableau suivant et sont également indiquées dans la rubrique *DSOP* avec une icône de changement.

Section/Sous-section	Description de la modification
Il n'y a aucun changement apporté à cette version.	

Que faire s'il y a un Incident touchant les Données?

Veuillez suivre les étapes suivantes si vous avez constaté un Incident touchant les Données dans votre entreprise.

Étape 1 :
Remplissez le Formulaire de départ du Marchand pour un Incident touchant les Données et envoyez-le par courriel à EIRP@aexp.com dans les 72 heures après la découverte de l'Incident touchant les Données.

Étape 2 :
Menez une enquête exhaustive. Cela peut demander que vous embauchiez un Enquêteur judiciaire du Secteur des cartes de paiement (SCP).

Étape 3 :
Fournissez-nous rapidement tous les Numéros des Cartes American Express® compromises.

Étape 4 :
Travaillez avec nous pour nous aider à résoudre tout problème découlant de l'Incident touchant les Données.

Consultez la Section 3, Obligations en matière de gestion des Incidents touchant les Données pour plus de détails quant aux obligations en matière d'Incidents touchant les Données.

Davantage de questions?

Numéro aux É.-U. : 888 732-3750 (sans frais)

International : +1 602 537-3021

EIRP@aexp.com

Chef de file en protection des consommateurs, American Express s'engage depuis longtemps à protéger et à garder confidentielles les Données des Titulaires de la Carte et les Données d'Authentification Sensibles.

L'atteinte à l'intégrité des données a un effet négatif sur les consommateurs, les Marchands, les Fournisseurs de services et les émetteurs de cartes. Un seul incident peut gravement nuire à la réputation d'une entreprise et l'empêcher de bien mener ses activités. Réagir face à cette menace en mettant en œuvre des Lignes directrices opérationnelles sur la sécurité peut aider à améliorer la confiance des clients, à accroître la rentabilité et à améliorer la réputation d'une entreprise.

American Express sait que nos Marchands et Fournisseurs de services (collectivement, **vous**) partagent ses préoccupations et que, dans le cadre de vos responsabilités, vous devez vous conformer aux dispositions sur la sécurité des données énoncées dans la Convention pour accepter (dans le cas des marchands) ou traiter (dans le cas des fournisseurs de services) la Carte American Express® (chacune respectivement, la **Convention**) et les présentes Lignes directrices opérationnelles sur la sécurité des données qui peuvent être modifiées de temps à autre. Ces exigences s'appliquent à votre matériel, à vos systèmes et à vos réseaux (de même qu'à leurs composants) sur lesquels des clés de chiffrement, des Données sur le Titulaire ou des Données d'Authentification Sensibles (ou une combinaison de celles-ci) sont conservées, traitées ou transmises.

Les termes clés utilisés dans les présentes qui n'y sont pas définis autrement ont le sens qui leur est donné dans le glossaire inclus à la fin des présentes lignes directrices.

Section 1 Programme d'analyse ciblée

La compromission des Données du Titulaire de la Carte peut être causée par des lacunes de votre Environnement des Données du Titulaire de Carte (EDTC).

Les exemples d'Incidents Touchant les Données des Titulaires de Cartes incluent, mais ne sont pas limités à ce qui suit :

- **Point d'achat commun (PAC) :** Les titulaires d'une Carte American Express signalent des Transactions frauduleuses sur leur compte, identifiées et déterminées comme ayant pour origine des achats effectués dans vos Établissements.
- **Données trouvées à propos de la Carte :** Les Données relatives aux Cartes American Express et à leurs Titulaires trouvées sur le Web et liées à des Transactions effectuées dans vos Établissements.
- **Logiciel malveillant :** American Express soupçonne que vous utilisez un logiciel infecté ou vulnérable à un code malveillant.

Le Programme d'analyse ciblée est conçu pour déterminer les possibles compromissions des données du Titulaire de Carte.

Vous devez vous conformer et faire en sorte que vos Tiers visés se conforment aux exigences suivantes dès le signalement par American Express d'une compromission possible des données du Titulaire de Carte.

- Vous devez rapidement examiner votre EDTC pour y déceler les lacunes en matière de sécurité des données et remédier à chacune d'entre elles.
  - Vous devez demander à votre/vos fournisseur(s) tiers de mener une enquête approfondie sur votre EDTC s'il est externalisé.
- Vous devez fournir un résumé des mesures prises ou prévues de vos efforts d'analyse, d'évaluation et (ou) de correction dès le signalement par American Express.
- Vous devez fournir des documents de validation de Normes du SCP mis à jour conformément à la Section 5, Importante validation périodique de vos systèmes.
- Le cas échéant, vous devez embaucher un Enquêteur judiciaire du SPC qualifié pour examiner votre EDTC si vous ou votre Tiers visé :
  - Ne pouvez pas résoudre la compromission des Données du Titulaire de Carte à l'intérieur d'une période raisonnable, comme déterminée par American Express, ou
  - Vous confirmez que l'Incident touchant les Données s'est produit et que vous vous conformez aux exigences établies à la Section 3, Obligations en matière de gestion des Incidents touchant les Données.

Tableau 1 : Frais de non-conformité au Programme d'analyse ciblée

Description	Marchand de niveau 1 ou Fournisseur de services de niveau 1	Marchand de niveau 2 ou Fournisseur de services de niveau 2	Marchand de niveau 3 ou 4
Des frais de non-conformité peuvent être imposés lorsque les obligations en vertu du Programme d'analyse ciblée ne sont pas satisfaite.	25 000 $ US	5 000 $ US	1 000 $ US
Des frais de non-conformité peuvent être imposés lorsque les obligations en vertu du Programme d'analyse ciblée ne sont pas satisfaites avant la deuxième échéance.	35 000 $ US	10 000 $ US	2 500 $ US
Des frais de non-conformité peuvent être imposés lorsque les obligations en vertu du Programme d'analyse ciblée ne sont pas satisfaites avant la troisième échéance. REMARQUE : *Les frais de non-conformité peuvent continuer à être appliqués jusqu'à ce que les obligations soient respectées, ou jusqu'à la résolution du Programme d'analyse ciblée.*	45 000 $ US	15 000 $ US	5 000 $ US

Si vos obligations relatives au Programme d'analyse ciblée ne sont pas respectées, American Express se réserve le droit d'imposer des frais de non-conformité cumulatifs, de retenir les paiements et (ou) de résilier la Convention.

Section 2 Normes de protection des Clés de chiffrement, des Données sur les Titulaires et des Données d'Authentification Sensibles

Vous devez faire, et vous assurer que vos Tiers visés fassent, ce qui suit :

- conserver les Données sur le Titulaire de la Carte American Express uniquement pour faciliter les Transactions, conformément à la Convention;
- vous conformer aux Normes de sécurité des données actuelles et autres exigences du Conseil des normes de sécurité des données du secteur des cartes de paiement (normes SCP) ou aux exigences relatives au traitement, à la conservation ou à la transmission des renseignements sur le Titulaire ou des Données d'authentification sensibles, au plus tard à la date d'entrée en vigueur de la mise en œuvre de cette version; et
- utiliser uniquement des Dispositifs de saisie du NIP ou des Applications de paiement (ou les deux) approuvés par le SCP lorsque ceux-ci sont ajoutés ou remplacés.

Conformément aux dispositions sur la sécurité des données, vous devez protéger tous les reçus d'Opération et les bordereaux de Crédit d'American Express conservés en vertu de la Convention, et vous devez utiliser ces reçus et ces bordereaux aux seules fins prévues à la Convention et les protéger en conséquence. En plus de démontrer que les parties visées se conforment à la présente politique en vertu de la Section 5, Importante validation périodique de vos systèmes, ci-dessous, sauf indication contraire dans ladite section, vous avez la responsabilité financière, ainsi que d'autres responsabilités à l'égard d'American Express de vous assurer que les parties visées respectent ces dispositions en matière de sécurité des données.

Section 3 Obligations en matière de gestion des Incidents touchant les Données

Vous devez aviser American Express immédiatement au moment de la découverte d'un Incident touchant les Données ou dans un délai maximum de soixante-douze (72) heures après la découverte de cet Incident.

Pour aviser American Express, veuillez communiquer avec l'EIRP (Enterprise Incident Response Program) d'American Express en composant le numéro sans frais 1 888 732-3750 ou le 1 602 537-3021, ou par courriel au EIRP@aexp.com. Vous devez désigner une personne-ressource à joindre en cas d'Incident touchant les Données. De plus :

- Vous devez effectuer une vérification judiciaire détaillée de chaque Incident touchant les Données.
- Dans le cas des Incidents touchant les Données mettant en cause au moins 10 000 Numéros uniques de Carte American Express (ou à la demande d'American Express), vous devez engager un Enquêteur judiciaire du SCP pour mener cette enquête dans les cinq (5) jours suivant la découverte d'un Incident touchant les Données.
- Le rapport de l'enquête judiciaire doit être fourni à American Express, sans modification, dans les dix (10) jours ouvrables suivant la rédaction.
- Vous devez rapidement fournir à American Express la liste de tous les Numéros de Cartes compromises. American Express se réserve le droit de mener sa propre analyse interne afin de déterminer quels Numéros de Carte ont été touchés par l'Incident concernant les Données.

Les Rapports de vérification judiciaire doivent être établis à l'aide du Modèle actuel de rapport d'enquête final, disponible auprès du SCP. Ce rapport doit comprendre les examens judiciaires, les rapports sur la conformité et tous les autres renseignements relatifs à l'incident touchant les données; c'est-à-dire que vous devez identifier la cause de l'incident touchant les données, confirmer que vous étiez conforme ou non aux normes du SCP au moment de l'incident touchant les données, confirmer votre engagement à prévenir tout autre incident touchant les données en (i) fournissant un plan de correction de toutes les lacunes relatives à ces normes et (ii) en participant au programme de conformité d'American Express (comme décrit ci-dessous). À la demande d'American Express, vous devez fournir une validation par un Évaluateur de sécurité qualifié (ÉSQ) attestant que les lacunes ont été comblées.

Nonobstant les paragraphes précédents de la présente Section 3, Obligations en matière de gestion des Incidents touchant les Données :

- American Express peut, à sa seule discrétion, vous demander de faire appel à un Enquêteur judiciaire du SCP pour enquêter sur un incident touchant les données pour les incidents impliquant moins de 10 000 Numéros de Carte uniques. Toute enquête de ce type doit se conformer aux exigences énoncées ci-dessus dans la présente Section 3, Obligations en matière de gestion des Incidents touchant les Données et doit être achevée dans les délais prescrits par American Express.
- American Express peut, à sa seule discrétion, engager séparément un Enquêteur judiciaire du SCP pour enquêter sur tout Incident touchant les Données et peut vous facturer le coût de cette enquête.

Vous devez collaborer avec American Express pour corriger tout problème découlant de l'Incident touchant les Données, y compris consulter American Express au sujet de vos communications avec les Titulaires de la Carte American Express touchés par l'Incident et fournir à American Express (et obtenir les renonciations nécessaires pour ce faire) les renseignements pertinents pour qu'il puisse vérifier votre capacité à prévenir tout autre Incident touchant les Données conformément à la Convention.

Nonobstant toute disposition contraire aux obligations de confidentialité énoncées dans la Convention, American Express a le droit de divulguer des renseignements au sujet de tout Incident concernant les Données aux Titulaires, aux Émetteurs, aux membres du Réseau d'American Express et au grand public, en vertu de la Loi en vigueur, d'un ordre judiciaire, administratif ou de réglementation, d'un décret, d'une assignation à témoigner, d'une demande ou de tout autre processus visant à réduire le risque de fraude ou de préjudice ou, dans la mesure du possible, à favoriser l'exploitation du Réseau d'American Express.

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

Vos obligations envers American Express en matière d'indemnisation en cas d'Incident touchant les Données dans le cadre de la Convention sont stipulées, sans restreindre les droits et les recours d'American Express, dans la présente Section 4, Obligations en matière d'indemnisation en cas d'Incident touchant les Données. En plus de vos obligations en matière d'indemnisation (le cas échéant), vous pouvez être sujet à des frais de non-conformité en cas d'Incident touchant les Données, comme décrit ci-dessous dans la présente Section 4, Obligations en matière d'indemnisation en cas d'Incident touchant les Données.

Pour les Incidents touchant les Données qui impliquent :

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

  vous indemniserez American Express au montant de 5 $ US par numéro de compte.

Toutefois, American Express ne vous demandera pas de l'indemniser pour un Incident impliquant touchant les Données :

- mettant en cause moins de 10 000 Numéros de Carte American Express, ou
- mettant en cause plus de 10 000 Numéros de Carte American Express, si vous remplissez les conditions suivantes :
  - vous avez avisé American Express de l'Incident touchant les Données en vertu de la Section 3 Obligations en matière de gestion des Incidents touchant les Données;
  - vous respectiez les normes du SCP au moment de l'Incident touchant les Données (tel que le démontre l'enquête effectuée par l'Enquêteur judiciaire du SCP sur l'incident touchant les données); et
  - l'Incident touchant les Données n'est pas le résultat d'un comportement fautif de votre part ou de la part d'un de vos Tiers visés.

Nonobstant les paragraphes précédents de la présente 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 devez payer à American Express des frais de non-conformité aux Incidents touchant les Données ne dépassant pas 100 000 $ US par Incident touchant les Données (déterminés par American Express, à sa seule discrétion) dans le cas où vous ne respectez pas l'une de vos obligations énoncées dans la Section 3, Obligations en matière de gestion des Incidents touchant les Données. Pour éviter tout doute, le total des frais de non-conformité des Incidents liés aux Données ne doit pas dépasser 100 000 $ US.

American Express exclura de son calcul tout Numéro de Compte de Carte American Express compromis qui a été inclus dans une demande d'indemnisation pour Incident touchant les Données antérieure que nous avons présentée dans les douze (12) mois précédant la Date de Notification. Tous les calculs effectués par American Express dans le cadre de cette méthode sont définitifs.

American Express pourrait vous facturer le plein montant de votre obligation d'indemnisation pour les Incidents touchant les Données, ou déduire le montant des paiements American Express qui vous sont destinés (ou débiter votre Compte bancaire pour ledit montant) selon la Convention.

Lorsqu'elles sont liées aux Incidents touchant les Données en vertu des présentes, vos obligations ne doivent pas être considérées comme des dommages accessoires, indirects, spéculatifs, consécutifs, spéciaux, punitifs ou exemplaires en vertu de la Convention ; à condition que ces obligations n'incluent pas les dommages liés à ou de la nature de la perte de profits ou de revenus, de la perte de clientèle ou de la perte d'occasions d'affaires.

American Express pourra, à son entière discrétion, réduire l'obligation d'indemnité pour les Marchands uniquement pour les Incidents touchant les Données découverts qui répondent à chacun des critères suivants :

- les Technologies applicables permettant de limiter les risques ont été utilisées avant l'Incident touchant les Données et étaient actives pendant toute la durée de l'Incident touchant les Données;

- une enquête approfondie, conforme au programme de l'enquêteur judiciaire du SCP a été complétée (sous réserve d'un autre accord préalable, rédigé);
- le rapport judiciaire indique clairement que les Technologies d'atténuation des risques ont été utilisées pour le traitement, le stockage et/ou la transmission des données au moment de l'Incident touchant les Données; et
- vous ne stockez pas – et n'avez pas stocké pendant la durée de l'Incident touchant les Données – de Données d'Authentification Sensibles ou de Données sur le Titulaire sans les avoir rendues illisibles.

Lorsqu'une réduction d'indemnisation est offerte, ladite réduction de votre obligation d'indemnisation (à l'exclusion de tous frais de non-conformité à payer) sera déterminée comme suit :

Tableau 2 : Critères relatifs à la réduction de l'obligation d'indemnisation

Réduction de l'obligation d'indemnisation	Critères requis
Réduction standard : 50 %	Plus de 75 % du total des Transactions traitées par des Dispositifs à puce[1] OU
	La Technologie d'atténuation des risques est utilisée dans plus de 75 % des emplacements des Marchands[2]
Réduction améliorée : 75 % à 100 %	Plus de 75 % des Transactions traitées par des Dispositifs à puce[1] ET une autre Technologie d'atténuation des risques sont utilisées dans plus de 75 % des emplacements de Marchands[2]

[1] Selon la détermination de l'analyse interne d'American Express
[2] Selon la détermination du programme de l'Enquêteur judiciaire

- La réduction accrue (de 75 % à 100 %) est déterminée selon le plus faible pourcentage des transactions traitées par des dispositif à puce ET les établissements du marchand utilisent une autre Technologie d'atténuation des risques. Les exemples ci-dessous illustrent le calcul de la réduction de l'indemnité.
- Pour être admissible à une Technologie d'atténuation des risques, vous devez démontrer l'utilisation effective de ladite technologie conformément à sa conception et à son usage prévu. À titre d'exemple, le déploiement de Dispositifs à puce et le traitement de Carte à puce en tant que Transaction par Bande Magnétique ou de saisie par touches ne constitue PAS une utilisation de cette technologie.
- Le pourcentage de vos établissements utilisant une Technologie d'atténuation des risques est déterminé par l'enquête réalisée par l'Enquêteur judiciaire.
- La réduction de l'obligation d'indemnisation ne s'applique à aucuns frais de non-conformité exigibles relatifs à l'Incident touchant les Données.

Tableau 3 : Réduction de l'obligation d'indemnisation accrue

Ex.	Technologie d'atténuation des risques utilisée	Admissibilité à la réduction accrue de l'obligation d'indemnisation	Réduction
1	80 % des Transactions par des Dispositifs à puce	Non	50 % : Réduction standard (une utilisation de moins de 75 % de Technologies d'atténuation des risques n'autorise pas une admissibilité à une réduction améliorée)[1]
	0 % des emplacements utilisent d'autres Technologies d'atténuation des risques		
2	80 % des Transactions par des Dispositifs à puce	Oui	77 % : Réduction améliorée (basé sur 77 % d'utilisation d'une

	77 % des emplacements utilisent d'autres Technologies d'atténuation des risques		Technologie d'atténuation des risques)
3	93 % des Transactions par des Dispositifs à puce	Oui	93 % : Réduction améliorée (basé sur 93 % de Transactions avec des Dispositifs à puce)
	100 % des emplacements utilisent d'autres Technologies d'atténuation des risques		
4	40 % des Transactions par des Dispositifs à puce	Non	50 % : Réduction standard (moins de 75 % de Transactions avec des Dispositifs à puce ne permettent pas une admissibilité à la réduction améliorée)
	90 % des emplacements utilisent d'autres Technologies d'atténuation des risques		

[1] Un Incident touchant les Données de 10 000 comptes-Cartes American Express à un taux de 5 $ US par numéro de compte (10 000 x 5 $ = 50 000 $ US) peut être admissible à une réduction de 50 %, réduisant l'obligation d'indemnisation de 50 000 $ à 25 000 $ US, excluant les frais de non-conformité.

Section 5 Importante validation périodique de vos systèmes

Vous devez effectuer les mesures décrites ci-dessous annuellement et trimestriellement, pour faire valider, selon les normes SCP, l'état de votre matériel, de vos systèmes et (ou) de vos réseaux (et de leurs composantes) qui servent à stocker, à traiter et à transmettre des données sur les titulaires de la Carte ou des Données d'authentification sensibles.

Quatre mesures sont nécessaires à la validation :

Mesure 1 : Participer au programme de conformité aux normes SCP d'American Express (« le Programme ») en vertu des présentes lignes directrices.

Mesure 2 : Comprendre votre Niveau de Marchand et les exigences de validation.

Mesure 3 : Remplir les Documents de validation à présenter à American Express.

Mesure 4: Faire parvenir les Documents de validation à American Express dans les délais prescrits.

Mesure 1 : Participer au Programme de conformité d'American Express en vertu des présentes Lignes directrices

Les Marchands de niveau 1 et de niveau 2, comme décrit ci-dessous, doivent participer au Programme en vertu des présentes lignes directrices. American Express peut désigner, à son entière discrétion, certains Marchands de Niveau 3 et de Niveau 4 pour participer au Programme en vertu de la présente politique.

Les Marchands et les Fournisseurs de services tenus de participer au Programme doivent s'inscrire au Portail fourni par l'administrateur du Programme choisi par American Express dans les délais prescrits.

- Vous devez accepter tous les termes et conditions raisonnables associés à l'utilisation du Portail.
- Vous devez attribuer et fournir des informations exactes pour au moins un contact de sécurité des données dans le Portail. Les éléments de données requis peuvent inclure :
  - nom complet
  - adresse électronique
  - numéro de téléphone

  - adresse postale principale
- Vous devez fournir des informations de contact actualisées ou nouvelles pour le contact désigné pour la sécurité des données dans le Portail lorsque ces informations changent.
- Vous devez vous assurer que vos systèmes sont mis à jour pour permettre les communications de service depuis le domaine désigné du Portail.

Le fait de ne pas maintenir les renseignements du contact de sécurité des données à jour n'affectera pas nos droits d'évaluer les frais de non-validation.

Mesure 2 : Comprendre votre Niveau de Marchand et les exigences de validation

Il existe quatre niveaux qui s'appliquent aux Marchands et deux niveaux pour les Fournisseurs de services, en fonction du volume de transactions que vous portez à la Carte American Express.

- Pour les Marchands, il s'agit du volume soumis par leurs Établissements qui s'élèvent au niveau le plus élevé du compte Marchand American Express.*
- Pour les Fournisseurs de services, il s'agit de la somme du volume soumis par le Fournisseur de services et les Entités prestataires de services auxquelles vous fournissez des services.

Les Transactions de paiement par l'acheteur (TPA) ne sont pas incluses dans le volume des Transactions de Cartes American Express pour déterminer les exigences de niveau de Marchand et de validation. Vous serez classé dans l'un des Niveaux de Marchand spécifiés dans les tableaux des Marchands et des Fournisseurs de services ci-dessous.

*Dans le cas des Franchiseurs, cela inclut le volume des Établissements de leurs Franchisés. Les Franchiseurs qui exigent que leurs Franchisés utilisent un Système de point de vente (PdV) ou un Fournisseur de services particulier doivent également fournir la documentation de validation pour les Franchisés concernés.

Exigences de Documents de validation du Marchand

Les Marchands (et non les Fournisseurs de services) ont quatre classifications possibles concernant leur Niveau. Après avoir déterminé le Niveau de Marchand dans la liste ci-dessous, consultez le Tableau 4 : Documents de validation du Marchand pour déterminer les exigences en matière de Documents de validation.

- **Marchand de niveau 1** – 2,5 millions de Transactions portées à la Carte American Express ou plus par année; ou tout Marchand qu'American Express estime, à sa seule discrétion, être de niveau 1.
- **Marchand de niveau 2** – De 50 000 à 2,5 millions de Transactions portées à la Carte American Express par année.
- **Marchand de niveau 3** – 10 000 à 50 000 Transactions portées à la Carte American Express par année.
- **Marchand de niveau 4** – Moins de 10 000 Transactions portées à la Carte American Express par année.

Tableau 4 : Documents de validation du Marchand

	Documents de validation		
Niveau de Marchand/ Transactions American Express annuelles	Rapport annuel d'attestation de conformité (ROC AOC)	Questionnaire attestation de conformité (SAQ AOC) ET Balayage trimestriel de la vulnérabilité du réseau externe (Balayage)	Attestation STEP pour les Marchands admissibles
Niveau 1/ 2,5 millions ou plus	Obligatoire	Sans objet	Facultatif avec l'autorisation d'American Express (remplace le Rapport d'évaluation de conformité)
Niveau 2/ 50 000 à 2,5 millions	Facultatif	SAQ AOC obligatoire (sauf si un ROC AOC est présenté); balayage obligatoire avec certains types de SAQ	Facultatif (remplace le SAQ et le balayage du réseau ou le Rapport d'évaluation de conformité sur place)
Niveau 3*/ 10 000 à 50 000	Facultatif	SAQ AOC facultatif (obligatoire si requis par American Express); balayage obligatoire avec certains types de SAQ	Facultatif (remplace le SAQ et le balayage du réseau ou le Rapport d'évaluation de conformité sur place)
Niveau 4*/ 10 000 ou moins	Facultatif	SAQ AOC facultatif (obligatoire si requis par American Express); balayage obligatoire avec certains types de SAQ	Facultatif (remplace le SAQ et le balayage du réseau ou le Rapport d'évaluation de conformité sur place)

*Pour éviter toute confusion, les Marchands de niveau 3 et de niveau 4 ne sont pas tenus de présenter des Documents de validation, à moins qu'American Express ne l'exige, à sa seule discrétion. Ils doivent toutefois respecter toutes les autres dispositions des Lignes directrices opérationnelles sur la sécurité des données et s'acquitter de leurs responsabilités en vertu de celles-ci.

American Express se réserve le droit de vérifier l'exhaustivité, l'exactitude et la pertinence des Documents de validation de SCP. American Express peut vous demander de fournir des pièces justificatives supplémentaires pour évaluation à l'appui de cette finalité. De plus, a le droit de vous demander d'engager un ÉSQ ou une Enquête judiciaire approuvée par le PCI Security Standards Council (Conseil sur les normes de sécurité du secteur des cartes de paiement).

Programme d'amélioration des technologies de sécurité (PATS)

Les marchands qui respectent les normes SCP peuvent, à la seule discrétion d'American Express, être admissibles au PATS d'American Express s'ils déploient certaines technologies de sécurité supplémentaires dans leurs Environnements de Traitement de Cartes. Un Marchand peut être admissible au PATS uniquement s'il n'a pas enregistré d'Incident touchant les Données au cours des 12 derniers mois et si 75 % de toutes ses Transactions par Carte sont traitées en utilisant une combinaison des options de sécurité renforcée suivantes :

- **EMV, EMV sans contact ou Portefeuille numérique** – sur un Dispositif à puce actif ayant une approbation/certification valide et actuelle EMVCo (www.emvco.com) et capable de traiter des Transactions par Carte à puce conformes aux normes PCPAE. (Les Marchands des États-Unis doivent inclure une Technologie sans contact)

- **Le chiffrement point à point (P2PE)** – communiquées à la société de traitement du marchand à l'aide d'un système de chiffrement point à point approuvé par le conseil des normes de sécurité du PCI ou par un ÉSQ
- **Authentification par jeton** – la solution de jeton d'authentification mise en oeuvre doit :
  - être conforme aux spécifications EMVCo,
  - être sécurisés, traités, stockés, transmis et entièrement gérés par un fournisseur de services tiers conforme aux normes SCP, et
  - le jeton d'authentification ne peut pas être inversé pour révéler les Numéros de compte primaire (NCP) non masqués au Marchand.

Les Marchands admissibles au PATS doivent se plier à moins d'exigences concernant les Documents de validation du SCP, tel que décrit en détail à la Mesure 3 : Remplir les Documents de validation à présenter à American Express ci-dessous.

Exigences pour le Fournisseur de services

Les Fournisseurs de services (pas les Marchands) ont deux classifications de Niveau possibles. Après avoir déterminé le Niveau de Fournisseur de services dans la liste ci-dessous, consultez le Tableau 5 : Documents pour le Fournisseur de services pour déterminer les exigences en matière de Documents de validation.

Fournisseur de services de niveau 1 – 2,5 millions ou plus de Transactions de Cartes American Express par année, ou tout Fournisseur de services considéré par American Express comme étant de niveau 1.

Fournisseur de services de niveau 2 – moins de 2,5 millions de Transactions de Cartes American Express par année ou tout Fournisseur de services considéré par American Express comme n'étant pas de niveau 1.

Les Fournisseurs de services ne sont pas admissibles au Programme PATS.

Tableau 5 : Documents pour le Fournisseur de services

Niveau	Documents de validation	Exigence
1	Rapport annuel d'attestation de conformité (ROC AOC)	Obligatoire
2	QAÉ annuelle D (Fournisseur de services) et Analyse de réseau trimestrielle ou Rapport annuel d'attestation de conformité (ROC AOC), si vous préférez	Obligatoire

Il est recommandé que les Fournisseurs de services se conforment également à la validation supplémentaire des entités désignées par le SCP.

Mesure 3 : Remplir les Documents de validation à présenter à American Express

Les documents suivants sont requis pour les différents niveaux de Marchands et de Fournisseurs de services énumérés dans le Tableau 4 : Documents de validation du Marchand et Tableau 5 : Documents pour le Fournisseur de services ci-dessus.

Vous devez fournir L'attestation de conformité (AOC) sur place pour le type d'évaluation applicable. L'AOC sur place est une déclaration de votre statut de conformité et, en tant que telle, doit être signée et datée par le niveau de direction approprié de votre organisation.

En plus de l'AOC, American Express peut vous demander de fournir une copie de l'évaluation complète et, à notre discrétion, des documents justificatifs supplémentaires démontrant la conformité aux exigences des normes SCP. Les documents de validation sont complétés à vos frais.

Rapport d'évaluation de conformité sur place (ROC AOC) - (exigence annuelle) – Le Rapport de conformité documente les résultats d'un examen détaillé sur place de vos équipements, systèmes et réseaux (et de leurs composants) où les Données des Titulaires de Cartes ou les Données d'Authentification Sensibles (ou les deux) sont stockées, traitées ou transmises. Il existe deux versions : Un pour les Marchands et un autre pour les Fournisseurs de service. Le Rapport sur la conformité doit être exécuté par :

- un ÉSQ; ou

- par vous et attestée par votre chef de la direction, chef des finances, chef de la sécurité de l'information ou mandant

L'AOC doit être signé et daté par un ÉSQ ou un Évaluateur de sécurité interne (ÉSI) et le niveau de direction autorisé au sein de votre organisation et fourni à American Express au moins une fois par an.

Questionnaire d'auto-évaluation Attestation de conformité (SAQ AOC) - (exigence annuelle) – Les questionnaires d'autoévaluation permettent l'autoexamen de vos équipements, systèmes et réseaux (et de leurs composants) dans lesquels des Données de Titulaires de Cartes ou des Données d'Authentification Sensibles (ou les deux) sont stockées, traitées ou transmises. Il existe plusieurs versions du questionnaire d'autoévaluation applicable. Vous en choisirez un ou plusieurs en fonction de votre Environnement de Données de Titulaire de Carte.

Le SAQ peut être rempli par le personnel de votre entreprise qualifié pour répondre aux questions de manière précise et approfondie ou vous pouvez faire appel à un ÉSQ pour vous aider. Le rapport annuel d'évaluation de conformité sur place doit être signé et daté par le niveau de direction autorisé au sein de votre organisation et fourni à American Express au moins une fois par an.

Fournisseur de balayage approuvé Résumé de l'analyse de vulnérabilité du réseau externe (Balayage FSBA) - (exigence chaque 90 jours) – Une analyse de vulnérabilité externe est un test à distance qui permet d'identifier les faiblesses, les vulnérabilités et les erreurs de configuration potentielles des composants de l'Environnement de Données des Titulaires de Cartes orientés vers l'Internet (p. ex., les sites Web, les applications, les serveurs Web, les serveurs de messagerie, les domaines orientés vers le public ou les hôtes).

Le Balayage FSBA doit être exécuté par un Fournisseur de services de balayage autorisé (FSBA).

Si la SAQ l'exige, l'attestation de conformité par balayage (AOSC) ou le résumé exécutif du rapport de balayage FSBA comprenant le nombre de cibles balayées, la certification que les résultats satisfont aux procédures de balayage SCP et le statut de conformité rempli par FSBA, doit être soumis à American Express au moins une fois tous les 90 jours.

Le ROC AOC ou PATS ne sont pas tenus de fournir un résumé exécutif de l'AOSC ou du balayage FSBA, sauf si spécifiquement requis. Pour éviter toute confusion, les Balayages sont obligatoires s'ils sont exigés par le questionnaire d'autoévaluation applicable.

Documents d'attestation de validation PATS (PATS) - (exigence annuelle) – PATS est seulement disponible aux Marchands qui satisfont les critères énumérés à la Mesure 2 : Comprendre votre Niveau de Marchand et les Documents de validation ci-haut. Si votre entreprise remplit les conditions requises, vous devez compléter le processus en présentant chaque année un formulaire d'Attestation PATS à American Express. Le document annuel d'attestation PATS peut être téléchargé du Portail.

Non-conformité aux normes SCP - (exigence annuelle, à tous les 90 jours, et (ou) ponctuelle) – Si vous n'êtes pas conforme aux normes SCP, vous devez présenter l'un des documents suivants :

- une Attestation de conformité (AOC) comprenant la « Partie 4. Plan d'action en cas de non-conformité » (disponible en téléchargement sur le site du conseil des normes de sécurité SCP)
- un résumé de l'outil d'approche prioritaire SCP (disponible en téléchargement sur le site du Conseil des normes de sécurité SCP)
- un modèle de plan de projet (accessible pour un téléchargement sur le Portail). Un plan de projet peut être soumis à la place de l'attestation annuelle (SAQ/ROC) et (ou) à la place de l'exigence de balayage.

Afin d'obtenir un statut de conformité, chacun des documents ci-dessus doit indiquer une date de correction qui ne dépasse pas les douze (12) mois suivant la date d'achèvement du document. Vous devez envoyer à American Express des mises à jour régulières de l'état d'avancement de l'ajustement dans le cadre de votre état de non-conformité (Marchands de niveau 1, 2, 3 et 4; tous les Fournisseurs de services). Les mesures nécessaires pour démontrer votre conformité aux normes SCP doivent être exécutées à vos frais.

American Express ne vous imposera pas de frais de non-validation (décrits ci-dessous) en raison de votre non-conformité avant la date d'ajustement, mais vous demeurez responsable à l'égard d'American Express pour

toutes les obligations d'indemnisation relatives à un Incident touchant les Données, en plus d'être assujetti à toutes les autres dispositions de la présente politique.

Pour éviter toute confusion, les marchands qui ne respectent pas les normes SCP ne sont pas admissibles au PATS.

Mesure 4 : Faire parvenir les Documents de validation à American Express

Tous les Marchands et Fournisseurs de services tenus de participer au Programme doivent présenter les Documents de validation identifiés comme étant « obligatoires » dans les tableaux de la Mesure 2 : Comprendre votre Niveau de Marchand et les Documents de validation à American Express dans les délais applicables.

Vous devez soumettre vos Documents de validation à American Express en utilisant le Portail fourni par l'administrateur du Programme sélectionné par American Express. En présentant les Documents de validation, vous déclarez et garantissez à American Express que ce qui suit est vrai (au mieux de vos connaissances) :

- Votre évaluation était complète et exhaustive;
- Le statut SCP est représenté de manière exacte au moment de l'achèvement, qu'il soit conforme ou non conforme;
- Vous êtes autorisé à divulguer les informations qu'il contient et vous fournissez la Documentation de validation à American Express sans violer les droits d'aucune autre partie.

Frais de non-validation et résiliation de la Convention

American Express a le droit de vous imposer des frais de non-validation et de résilier la Convention si vous ne répondez pas aux présentes exigences ou si vous ne transmettez pas à American Express les Documents de validation exigés dans les délais prescrits. American Express tentera d'informer la personne-ressource chargée de la sécurité des données de toute échéance applicable pour chaque période de déclaration annuelle et trimestrielle.

Tableau 6 : Frais de non-validation

Description	Marchand de niveau 1 ou Fournisseur de services de niveau 1	Marchand de niveau 2 ou Fournisseur de services de niveau 2	Marchand de niveau 3 ou 4
Des frais de non-validation seront imposés si les Documents de validation ne sont pas reçus à la première échéance.	25 000 $ US	5 000 $ US	50 $ US
Des frais de non-validation supplémentaires seront imposés si les Documents de validation ne sont pas reçus avant la deuxième échéance.	35 000 $ US	10 000 $ US	100 $ US

Des frais de non-validation supplémentaires seront imposés si les Documents de validation ne sont pas reçus avant la troisième échéance. **REMARQUE :** Les frais de non-conformité seront imposés jusqu'à ce que les Documents de validation soient présentés.	45 000 $ US	15 000 $ US	250 $ US

Si vos obligations relatives aux Documents de validation des normes SCP ne sont pas respectées, American Express se réserve le droit d'imposer des frais de non-conformité cumulatifs, de retenir les paiements et (ou) de résilier la Convention.

Section 6

American Express prendra des mesures raisonnables pour garder (et faire en sorte que ses agents et sous-traitants, y compris le fournisseur du Portail, gardent) confidentiels vos rapports sur la conformité en toute confiance, y compris les Documents de validation et ne pas divulguer les documents de validation à un tiers (autres qu'aux Sociétés affiliées, mandataires, représentants, fournisseurs de services et sous-traitants d'American Express) pendant les trois (3) années qui suivent leur réception, à moins que cette obligation de confidentialité ne s'applique pas aux Documents de validation pour les raisons suivantes :

a. les documents étaient déjà connus d'American Express avant d'être divulgués;

b. les documents sont ou sont devenus accessibles au public sans qu'American Express ne viole les dispositions du présent alinéa;

c. un tiers a transmis les documents de validation de façon légitime à American Express, sans obligation de les garder confidentiels;

d. les documents de validation sont produits de façon indépendante par American Express; ou

e. les documents doivent être divulgués en vertu d'une ordonnance d'un tribunal, d'un organisme administratif ou d'une autorité gouvernementale, d'une loi, d'une règle ou d'un règlement, d'une citation à comparaître, d'une demande de communication préalable, d'une assignation, de toute autre procédure judiciaire ou administrative, ou encore d'une demande ou d'une enquête formelle ou informelle d'une agence ou d'un organisme gouvernemental (y compris un organisme de réglementation, un inspecteur, un auditeur ou un organisme d'application de la loi).

Section 7 Avis de non-responsabilité

AMERICAN EXPRESS SE DÉGAGE PAR LES PRÉSENTES DE TOUTES DÉCLARATIONS, GARANTIES ET RESPONSABILITÉS RELATIVES AUX PRÉSENTES EXIGENCES SUR LA SÉCURITÉ DES DONNÉES, AUX NORMES DE SÉCURITÉ DES DONNÉES DU SECTEUR DES CARTES DE PAIEMENT, AUX SPÉCIFICATIONS EMV ET À LA DÉSIGNATION ET AU RENDEMENT ÉSQ, DES FSBA OU DES ENQUÊTEURS JUDICIAIRES DU SCP (OU N'IMPORTE LEQUEL D'ENTRE EUX), QUE CELLES-CI SOIENT EXPLICITES, IMPLICITES, STATUTAIRES OU AUTRES, Y COMPRIS TOUTE GARANTIE RELATIVE À LA QUALITÉ MARCHANDE OU À L'ADAPTATION À UNE FIN PARTICULIÈRE. LES ÉMETTEURS DE CARTE AMERICAN EXPRESS NE SONT PAS DES TIERS BÉNÉFICIAIRES AUX TERMES DES PRÉSENTES LIGNES DIRECTRICES.

Sites Web utiles

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

PCI Security Standards Council, LLC (Conseil sur les normes de sécurité du secteur des cartes de paiement, s.r.l.) : www.pcisecuritystandards.org

Glossaire

Aux fins des présentes lignes directrices seulement, les définitions suivantes s'appliquent :

Application de paiement a la signification donnée dans le glossaire en vigueur des Logiciels sécurisés et des normes de cycle de vie des Logiciels sécurisés accessibles sur le site www.pcisecuritystandards.org.

Approuvé par le secteur des cartes de paiement désigne un Dispositif de saisie du NIP ou une Application de paiement (ou les deux) qui est ajouté au moment de la mise en place sur la liste des entreprises et des fournisseurs autorisés tenue par le PCI Security Standards Council, LLC (Conseil des normes de sécurité des données du secteur des cartes de paiement, s.r.l.), que l'on trouve à l'adresse www.pcisecuritystandards.org.

Attestation de conformité (AOC) désigne une déclaration de votre niveau de conformité aux normes SCP, présentée sur un formulaire fourni par le Payment Card Industry Security Standards Council, LLC (Conseil sur les normes de sécurité des données du secteur des cartes de paiement, s.r.l.).

Attestation de conformité par balayage (AOSC) désigne la déclaration de votre niveau de conformité aux normes SCP, fondée sur un balayage et présentée sur un formulaire fourni par le Payment Card Industry Security Standards Council, LLC (Conseil des normes de sécurité des données du secteur des cartes de paiement, s.r.l.).

Carte American Express, ou Carte, désigne toute carte, tout dispositif d'accès au compte ou tout dispositif ou service de paiement portant le nom, le logo, la marque de commerce, la marque de service, le nom commercial ou tout autre logo ou désignation exclusive d'American Express ou d'une société affiliée et émis par un émetteur; ou un numéro de compte de carte.

Carte à puce désigne une Carte qui contient une Puce et qui pourrait nécessiter un numéro d'identification personnel (NIP) comme moyen pour vérifier l'identité du Titulaire, l'information sur le compte que la Puce renferme ou les deux (parfois appelée « carte intelligente », « Carte EMV », « ICC » ou « carte à puce intégrée » dans nos documents).

Chiffrement point-à-point (P2PE) désigne une solution qui protège cryptographiquement les données du compte à partir du point où un marchand accepte la carte de paiement jusqu'au point de décryptage sécurisé.

Clé de chiffrement (clé de chiffrement American Express) désigne toute clé utilisée pour le traitement, la production, le chargement et (ou) la protection des Données du Compte. Cela comprend notamment ce qui suit :

- Principales clés de chiffrement : Clés principales de contrôle de zone (ZMK) et clés de NIP de zone (ZPK)
- Clés principales utilisées dans les dispositifs de chiffrement : Clés principales locales (LMK)
- Clés de code de sécurité de la Carte (CSCK)
- Clés de NIP : Clés de dérivation de base (BDK), Clés de chiffrement NIP (PEK) et ZMK

Crédit désigne le montant d'Opération que vous remboursez à un Titulaire relativement à un achat ou à un paiement porté à la Carte.

Date de notification désigne la date à laquelle American Express fournit aux émetteurs un dernier avis d'Incident touchant les Données. Cette date est conditionnelle à la réception par American Express du rapport d'enquête final ou de l'analyse interne, et est déterminée à la seule discrétion d'American Express.

Dispositif à puce désigne un dispositif de point de vente avec une approbation/attestation EMVCo valide et à jour (www.emvco.com) et en mesure de traiter des opérations par Cartes à puce conformes aux spécifications PCPAE.

Dispositif de saisie du NIP a le sens défini dans le glossaire alors en vigueur des exigences relatives à la sécurité des Transactions avec NIP du secteur des cartes de paiement en ce qui concerne les points d'interaction et les exigences de sécurité modulaire, que l'on trouve à l'adresse www.pcisecuritystandards.org.

Document de validation désigne l'Attestation de conformité fournie à l'égard de la vérification annuelle de la sécurité sur place ou du Questionnaire d'autoévaluation, de l'Attestation de conformité du balayage de réseau et du sommaire des résultats fourni en lien avec le Balayage trimestriel du réseau ou l'Attestation annuelle du PATS.

Données d'authentification sensibles a la signification donnée dans le glossaire en vigueur des termes du SCP.

Données sur le titulaire a le sens défini dans le glossaire alors en vigueur des normes SCP.

Émetteur désigne toute entité (y compris American Express et ses Sociétés affiliées) autorisée par American Express ou une société affiliée d'American Express à émettre des Cartes et à exercer l'activité d'émission de Cartes.

Enquêteur judiciaire du SCP désigne une entité approuvée par le conseil sur les normes de sécurité du secteur des cartes de paiement, une société à responsabilité limitée, pour procéder à la vérification judiciaire de la brèche ou de la compromission des données d'une carte de paiement.

Environnement des Données du Titulaire de Carte (EDTC) désigne les gens, les processus et la technologie qui entrepose, traite et transmet les données du Titulaire de carte ou les données de nature délicate d'authentification.

Exigences de sécurité concernant le NIP du SCP désigne les exigences de sécurité concernant le NIP du secteur des cartes de paiement, accessibles à l'adresse www.pcisecuritystandards.org.

Exigences du Conseil des normes de sécurité des données du secteur des cartes de paiement (normes SCP) désigne l'ensemble des normes et exigences relatives à la sécurisation et à la protection des données des cartes de paiement, y compris les normes SCP, accessibles à www.pcisecuritystandards.org.

Évaluateur de sécurité qualifié (ÉSQ) désigne une entité accréditée par le Payment Card Industry Security Standards Council, LLC (Conseil des normes de sécurité des données du secteur des cartes de paiement, s.r.l.) pour vérifier la conformité à ses normes.

Fenêtre de l'Incident touchant les Données désigne la période de compromission (ou une période similaire déterminée) établie dans le rapport judiciaire définitif (p. ex. rapport d'ÉSQ), ou si la période est inconnue, jusqu'à 365 jours avant la dernière Date de notification de la possible compromission des numéros de Carte impliqués dans la compromission des données qui nous a été signalée.

Fournisseurs de services désigne les sociétés de traitement, sociétés de traitement indépendantes, fournisseurs de passerelle, intégrateurs de Systèmes de PdV et tout autre fournisseur aux Marchands de Systèmes de PdV ou d'autres solutions ou services de traitement des paiements.

Fournisseur de services de balayage autorisés (FSBA) désigne une entité accréditée par le Payment Card Industry Security Standards Council, LLC (Conseil des normes de sécurité des données du secteur des cartes de paiement, s.r.l.) pour vérifier la conformité à certaines exigences découlant de ces normes (SCP), au moyen d'évaluations de la vulnérabilité des systèmes électroniques (sur Internet).

Fournisseur de services de niveau 1 désigne un Fournisseur de services compilant 2,5 millions ou plus de Transactions de Cartes American Express par année, ou tout Fournisseur de services considéré par American Express comme étant de niveau 1.

Fournisseur de services de niveau 2 désigne un Fournisseur de services compilant moins de 2,5 millions de Transactions de Cartes American Express par année ou tout Fournisseur de services considéré par American Express comme n'étant pas de niveau 1.

Franchisé désigne un propriétaire-exploitant indépendant (y compris un franchisé, un titulaire de licence ou une branche), autre qu'une des Sociétés membres du groupe, à qui un Franchiseur accorde une licence pour exploiter une Franchise et qui a signé une convention écrite avec le Franchiseur lui permettant d'afficher des Marques d'identification externe, de se présenter de façon constante avec les marques du franchiseur et de se présenter comme une des sociétés membres du groupe du Franchiseur.

Franchiseur désigne l'exploitant d'une entreprise qui accorde à des personnes ou à des Entités (Franchisés) une licence pour distribuer des biens et (ou) des services sous sa Marque ou pour opérer en utilisant sa marque; qui fournit une assistance aux Franchisés dans l'exploitation de leur entreprise ou qui influence le mode d'exploitation du Franchisé; et qui exige le paiement d'une redevance par les Franchisés.

Incident touchant les Données désigne un incident mettant en cause ou soupçonné de mettre en cause une clé de chiffrement American Express ou au moins un numéro de compte-Carte American Express pour lequel il y a :

- une utilisation ou un accès non autorisé des Clés de chiffrement, des Données sur les Titulaires ou des Données d'Authentification Sensibles (ou une combinaison de ces éléments) qui sont conservées, traitées ou transmises par l'équipement et les systèmes et (ou) les réseaux (ou leurs composants) qui vous appartiennent ou dont vous mandatez l'utilisation, fournissez ou rendez disponibles;
- l'utilisation de ces Clés de chiffrement, de ces Données sur le Titulaire ou de ces Données d'Authentification Sensibles (ou une combinaison de ces éléments) autre que celle qui respecte la Convention; et (ou)
- une perte, une appropriation indue ou un vol, confirmé ou soupçonné, par tout moyen, du média, de la clause, du dossier ou de l'information où sont contenues les Clés de chiffrement, les Données sur les Titulaires ou les Données d'Authentification Sensibles (ou une combinaison de ces éléments).

Jeton d'authentification désigne le jeton cryptographique qui remplace le Numéro du compte principal (NCP), sur la base d'un indice donné pour une valeur imprévisible.

Marchand désigne le Marchand et toutes ses sociétés affiliées acceptant les Cartes American Express dans le cadre d'une convention avec American Express ou ses Sociétés affiliées.

Marchand de niveau 1 désigne un Marchand compilant 2,5 millions ou plus de Transactions de Cartes American Express par année, ou tout Marchand autrement considéré par American Express comme un Marchand de niveau 1.

Marchand de niveau 2 désigne un Marchand compilant de 50 000 à 2,5 millions de Transactions portées à la Carte American Express par année.

Marchand de niveau 3 désigne un Marchand compilant de 10 000 à 50 000 Transactions portées à la Carte American Express par année.

Marchand de niveau 4 désigne un Marchand compilant moins de 10 000 Transactions portées à la Carte American Express par année.

Modèle de rapport final de l'enquête judiciaire sur l'incident désigne le modèle du Conseil des normes de sécurité du SCP, accessible sur le site www.pcisecuritystandards.org.

Niveau de Marchand désigne le classement des Marchands en fonction du respect de leurs obligations en matière de leur conformité aux normes SCP du PCI, telles qu'elles sont énoncées à la Section 5 Importante validation périodique de vos systèmes.

Normes de sécurité des données de l'industrie des cartes de paiement (Normes SCP) désigne les normes de sécurité des données de l'industriel disponibles à https://www.pcisecuritystandards.org.

Normes SCP désigne les normes de sécurité des données du secteur des cartes de paiement, accessibles à l'adresse www.pcisecuritystandards.org.

Numéro de Carte désigne le numéro d'identification unique que l'Émetteur attribue à une Carte au moment où elle est émise.

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

Numéro du compte principal (NCP) a le sens défini dans le glossaire alors en vigueur des normes SCP.

Opération désigne un paiement ou un achat effectué avec la Carte.

Portail, Le désigne le système de rapport fourni par l'administrateur du Programme SCP d'American Express choisi par American Express. Les Marchands et les Fournisseurs de services sont doivent utiliser le Portail pour présenter les Documents de validation de SCP à American Express.

Processeur désigne un fournisseur de services aux Marchands qui facilite les processus d'autorisation et de soumission pour le réseau d'American Express.

Programme d'amélioration des technologies de sécurité (PATS) désigne le programme d'American Express dans le cadre duquel les marchands sont encouragés à déployer des technologies qui renforcent la sécurité des données.

Programme d'analyse ciblée est un programme qui fournit une détermination hâtive d'une compromission possible des données du Titulaire de Carte dans votre EDTC. Programme d'analyse ciblée.

Programme, Le désigne le Programme de conformité aux normes SCP American Express.

Puce désigne une micropuce intégrée à une Carte et sur laquelle sont enregistrés des renseignements sur le titulaire et le compte-Carte.

Questionnaire d'autoévaluation (QAÉ) désigne un outil d'autoévaluation conçu pour les marchands par le Payment Card Industry Security Standards Council, LLC. (Conseil des normes de sécurité des données du secteur des cartes de paiement, s.r.l.), afin qu'ils évaluent et attestent leur conformité aux normes SCP du PCI.

Renseignements sur un Titulaire désigne les informations relatives aux Titulaires de Cartes American Express et aux Transactions par Carte, y compris les noms, adresses, numéros de compte carte et numéros d'identification de la carte (NIC).

Société de traitement désigne un fournisseur de services aux Marchands qui facilite les processus d'autorisation et de soumission pour le réseau d'American Express.

Solution de chiffrement point à point (P2PE) approuvée, incluse dans la liste de solutions validées par le conseil des normes de sécurité du PCI ou par une entreprise agissant à titre d'Évaluateur de sécurité qualifié.

Spécifications EMV désigne les spécifications émises par EMVCo, LLC qui sont disponibles à www.emvco.com.

Technologie d'atténuation des risques désigne les solutions technologiques qui, selon la détermination d'American Express, améliorent la sécurité des Données des Titulaires de Carte American Express et des Données d'Authentification Sensibles. Pour être admissible à une Technologie d'atténuation des risques, vous devez démontrer l'utilisation effective de ladite technologie conformément à sa conception et à son usage prévu. Les exemples comprennent, mais ne sont pas limités à : Spécifications EMV, cryptage point à point et jeton d'authentification.

Terminal point de vente (PdV) désigne un terminal ou matériel de traitement des données, par exemple un terminal, un ordinateur personnel, une caisse enregistreuse électronique, un lecteur sans contact ou un processus ou mécanisme de paiement, que le Marchand utilise pour obtenir une autorisation ou saisir les données sur la Transaction, ou les deux.

Tiers visés désigne l'ensemble de vos employés, agents, représentants, sous-traitants, Sociétés de traitement, Fournisseurs de services, ou fournisseurs de matériel ou de systèmes point de vente (PdV) ou de solutions de traitement des paiements, les Entités associées à votre compte Marchand d'American Express, et toute autre partie à laquelle vous donnez un accès aux Données des Titulaires ou aux Données d'Authentification Sensibles (ou les deux) conformément à la Convention.

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

Transaction désigne une Opération ou Crédit réalisé au moyen de la Carte.

Transactions de paiement par l'acheteur (TPA) désigne une opération de paiement activée par un fichier d'instructions de paiement traité par TPA.

Transaction par EMV désigne une Transaction effectuée au moyen d'une Carte à puce intégrée (parfois appelée « carte IC », « carte à puce », « carte intelligente », « carte EMV » ou « ICC ») sur un terminal de point de vente (PdV) adapté aux cartes à circuit intégré présentant une approbation d'EMVCo valide et à jour. Les types d'approbations d'EMVCo sont indiqués à l'adresse www.emvco.com.