AMERICAN EXPRESS

Lignes directrices opérationnelles sur la sécurité des données

AMERICAN EXPRESS

Résumé des modifications des Lignes directrices opérationnelles sur la sécurité des données

Icônes

Les mises à jour importantes sont répertoriées dans le Tableau de résumé des modifications et sont également indiquées dans les *Lignes directrices opérationnelles sur la sécurité des données* avec une barre de changement. Une barre de changement est une ligne verticale, généralement située dans la marge de gauche, qui désigne un passage ajouté ou révisé. Seules les modifications importantes dans les *Lignes directrices opérationnelles sur la sécurité des données* pouvant avoir des répercussions sur les procédures opérationnelles des marchands sont indiquées par une barre de changement 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 Résumé 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 de résumé des modifications

Les mises à jour importantes sont énumérées dans le tableau suivant et sont également indiquées dans les *Lignes directrices opérationnelles sur la sécurité des données* par une barre de changement.

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

Section 1 Introduction aux Lignes directrices opérationnelles sur la sécurité des données et aux normes de protection

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[MD] (chacune respectivement, la **Convention**) et les présentes Lignes directrices opérationnelles sur la sécurité des données (DSOP) qui peuvent être modifiées de temps à autre. Ces exigences s'appliquent à votre matériel, à vos systèmes et à vos réseaux (ainsi 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 ces éléments) 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.

Les Lignes directrices opérationnelles sur la sécurité des données se composent 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 marchands et fournisseurs de services respectent les normes de sécurité des données dans le secteur des cartes de paiement (normes SCP). Dans le cadre de cette exigence, 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 clés de chiffrement, 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.
- S'assurer d'utiliser des produits approuvés par le secteur des cartes de paiement pour déployer ou remplacer la technologie de stockage, traitement ou transmission des données.

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. Vous êtes responsable envers American Express, financièrement et autrement, de vous assurer de la conformité de vos tiers visés à l'égard des présentes dispositions sur la sécurité des données (autrement que pour prouver la conformité de vos tiers visés avec les présentes lignes directrices en vertu de la Section 2, « Programme de conformité aux normes SCP (Importante validation périodique de vos systèmes) », sauf stipulation contraire dans cette section). Des informations détaillées concernant les normes SCP et la conformité à leurs exigences sont disponibles sur le site www.pcisecuritystandards.org.

Section 2 Programme de conformité aux normes SCP (Importante validation périodique de vos systèmes)

Chaque 90 jours et chaque année, vous devez effectuer les mesures décrites ci-dessous pour faire valider, selon les normes SCP, l'état de votre matériel, de vos systèmes et (ou) de vos réseaux (et de leurs composantes) (et ceux de vos franchisés) 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 en vertu des présentes lignes directrices.
- Mesure 2 : Comprendre votre niveau de marchand/fournisseur de services et les documents de validation à fournir.
- 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, et tous les fournisseurs de services, comme décrit ci-dessous, doivent participer au Programme en vertu de la présente politique. 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 incluent :
  - nom complet
  - adresse électronique
  - numéro de téléphone
  - adresse postale physique
- 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 fournir ou maintenir à jour les renseignements du contact de sécurité des données ou de ne pas autoriser les communications par courrier électronique n'affectera pas nos droits d'évaluer les frais.

Mesure 2 : Comprendre votre niveau de marchand/fournisseur de services et les documents de validation à fournir

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 par Cartes American Express pour déterminer le niveau du marchand et les exigences de validation. Vous serez

classé dans l'un des niveaux de marchand spécifiés dans le Tableau 2-1 : Niveaux de marchand et de fournisseur de services.

* 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.

Tableau 2-1 : Niveaux de marchand et de fournisseur de services

Niveau de marchand fournisseur	Transactions American Express annuelles
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 moins de 2,5 millions de transactions portées à la Carte American Express par année.
Marchand de niveau 3	De 10 000 à moins de 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.
Niveau de fournisseur de services	**Transactions American Express annuelles**
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.

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 le Tableau 2-1 : Niveaux de marchand et de fournisseur de services (ci-dessus), voir le Tableau 2-2 : Documents de validation du marchand pour déterminer les exigences à respecter en matière de documents de validation.

Tableau 2-2 : Documents de validation du marchand

Niveau de marchand/ Transactions American Express annuelles	Rapport d'attestation de conformité (ROC AOC)	Questionnaire d'autoévaluation Attestation de conformité (SAQ AOC) ET Balayage trimestriel de la vulnérabilité du réseau externe (Balayage)	Attestation du programme d'amélioration des technologies de sécurité (PATS) 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 moins de 2,5 millions	Facultatif	SAQ AOC obligatoire (sauf si un rapport d'attestation de conformité est présenté); balayage obligatoire avec certains types de SAQ	Facultatif avec l'autorisation d'American Express* (remplace le SAQ et le balayage du réseau ou le ROC)
Niveau 3**/ 10 000 à moins de 50 000	Facultatif	SAQ AOC facultatif (obligatoire si requis par American Express); balayage obligatoire avec certains types de SAQ	Facultatif avec l'autorisation d'American Express* (remplace le SAQ et le balayage du réseau ou le ROC)
Niveau 4**/ Moins de 10 000	Facultatif	SAQ AOC facultatif (obligatoire si requis par American Express); balayage obligatoire avec certains types de SAQ	Facultatif avec l'autorisation d'American Express* (remplace le SAQ et le balayage du réseau ou le ROC)

* **Remarque :** L'équipe SCP d'American Express examinera la demande et l'admissibilité, et confirmera si vous remplissez les critères de participation au Programme PATS. Veuillez prendre contact avec votre gestionnaire des relations avec la clientèle et (ou) AXPPCIComplianceProgram@aexp.com pour vérifier les conditions d'admissibilité.

**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, American Express a le droit de vous demander d'engager un évaluateur de sécurité qualifié (ÉSQ) ou un enquêteur judiciaire approuvé par le PCI Security Standards Council (Conseil sur les normes de sécurité du secteur des cartes de paiement).

Exigences de documents de validation du 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 le Tableau 2-1 : Niveaux de marchand et de fournisseur de services (ci-dessus), consultez le Tableau 2-3 : Documents de validation du fournisseur de services pour déterminer les exigences à respecter en matière de documents de validation.

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

Tableau 2-3 : Documents de validation du fournisseur de services

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

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

Programme d'amélioration des technologies de sécurité (PATS)

Les marchands qui respectent les normes SCP peuvent aussi, 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)** – communiqué 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 SCP ou par un ÉSQ qualifié
- **Authentification par jeton** – la solution de jeton d'authentification mise en œuvre doit :
  - être conforme aux spécifications EMVCo,
  - être sécurisée, traitée, stockée, transmise et entièrement gérée 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.

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 2-2 : Documents de validation du marchand et le Tableau 2-3 : Documents de validation du fournisseur de services ci-dessus.

Vous devez fournir l'attestation de conformité (AOC) pour le type d'évaluation applicable. L'AOC 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'attestation de conformité (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 executé par :

- un ÉSQ; ou
- un évaluateur de sécurité interne (ÉSI) et attesté par votre chef de la direction, chef des finances, chef de la sécurité de l'information ou mandant

Le rapport d'attestation de conformité (ROC AOC) doit être signé et daté par un ÉSQ ou 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 (SAQ). 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 SAQ AOC 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 trimestrielle) – 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 le 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.

Si vous soumettez un rapport d'attestation de conformité (ROC AOC) ou PATS, vous n'êtes pas tenu 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 (SAQ) 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/ fournisseur de services et les documents de validation à fournir » ci-dessus. 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 formulaire d'attestation annuelle PATS peut être téléchargé par le biais du Portail. Vous pouvez également prendre contact avec votre gestionnaire des relations avec la clientèle ou écrire à American Express à l'adresse AXPPCIComplianceProgram@aexp.com.

Non-conformité aux normes SCP - (exigence annuelle, chaque 90 jours, et (ou) ponctuelle) – si vous n'êtes pas conforme aux normes SCP, vous devez présenter un résumé de l'outil d'approche prioritaire SCP (disponible en téléchargement sur le site du Conseil des normes de sécurité SCP).

Le résumé de l'outil d'approche prioritaire SCP doit désigner une date de correction sans dépasser 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 n'imposera pas de frais de non-conformité avant la date de correction. Conformément au Tableau 2-4 : 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 ces lignes directrives.

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

- un modèle d'approche prioritaire SCP n'a pas été soumis conformément aux exigences stipulées dans cette section;
- les étapes de correction décrites dans le modèle d'approche prioritaire SCP pour l'état de non-conformité n'ont pas été respectées;
- l'une des exigences du modèle d'approche prioritaire SCP 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 marchands/fournisseurs de services qui ne respectent pas les exigences stipulées dans la Mesure 2 : Comprendre votre niveau de marchand/fournisseur de services et les documents de validation à fournir, peuvent être soumis à des frais comme indiqué dans la Mesure 4 : Faire parvenir les documents de validation à American Express.

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/fournisseur de services et les documents de validation à fournir » 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 s'agisse de la soumission de l'attestation de conformité (AOC) ou d'un résumé de l'outil d'approche prioritaire SCP pour non-conformité;
- 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-conformité et résiliation de la Convention

American Express a le droit de vous imposer des frais de non-conformité 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 2-4 : Frais de non-conformité

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 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-conformité 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-conformité 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

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

* Non applicable en Argentine.

Si vos obligations relatives aux documents de conformité aux 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 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, contactez le Programme d'intervention de l'entreprise en cas d'incident d'American Express (Enterprise Incident Response Program) (*EIRP*) 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 enquête détaillée de chaque incident touchant les données et rapidement fournir à American Express tous les numéros de Cartes compromises. American Express se réserve le droit de mener sa propre analyse interne afin de déterminer quelles données ont été touchées par l'incident concernant 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.

Dans le cas des incidents touchant les données mettant en cause au moins 10 000 numéros uniques de Carte 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.
- 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 son entière 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 ou lorsque plusieurs incidents se sont produits au cours d'une période de 12 mois. 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 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 fournisseur de services ou à une autre entité de signaler l'incident touchant les données, vous devez informer ce fournisseur 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 devez collaborer avec American Express pour fournir des détails et corriger tout problème découlant de l'incident touchant les données, y compris fournir à American Express (et obtenir les renonciations nécessaires pour ce faire) les renseignements pertinents pour 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 des lois 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.

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 à l'intention des marchands pour le 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 du SCP (secteur des cartes de paiement).

Étape 3 :

Nous fournir immédiatement tous les numéros de Carte American Express[MD] compromis.

Étape 4 :

Collaborer avec nous afin de corriger tout problème résultant de l'incident touchant les données.

Consulter la Section 3, « Obligations en matière de gestion des incidents touchant les données » pour de plus amples informations sur les obligations en matière de gestion des incidents touchant les données.

Des questions?

États-Unis : +1 888 732-3750 (numéro sans frais)

International : +1 (602) 537-3021

EIRP@aexp.com

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 ».

Vous indemniserez American Express au montant de 5 $ US par numéro de compte, 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

Toutefois, American Express ne vous demandera pas de l'indemniser pour un incident touchant les données mettant en cause :

- 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 avisé American Express de l'incident touchant les données en vertu de la présente 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 imposés pour tout incident touchant les 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 vos obligations 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 concernant 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 l'accord; 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 de l'indemnité est disponible, la réduction de votre obligation d'indemnisation (à l'exclusion de tous frais de non-conformité à payer) sera déterminée comme suit :

Tableau 2-5 : Critères de 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 améliorée (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 dans le Tableau 2-6 : Réduction améliorée de l'obligation d'indemnisation illustrent le calcul de la réduction de l'indemnisation.
- 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.
- 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 2-6 : Réduction améliorée de l'obligation d'indemnisation

Ex.	Technologie d'atténuation des risques utilisée	Admissible	Réduction
1	• 80 % des transactions par des dispositifs à puce • 0 % des emplacements utilisent d'autres technologies d'atténuation des risques	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]
2	• 80 % des transactions par des dispositifs à puce • 77 % des emplacements utilisent d'autres technologies d'atténuation des risques	Oui	77 % : Réduction améliorée (basé sur 77 % d'utilisation d'une technologie d'atténuation des risques)
3	• 93 % des transactions par des dispositifs à puce • 100 % des emplacements utilisent d'autres technologies d'atténuation des risques	Oui	93 % : Réduction améliorée (basé sur 93 % de transactions avec des dispositifs à puce)

Tableau 2-6 : Réduction améliorée de l'obligation d'indemnisation (suite)

Ex.	Technologie d'atténuation des risques utilisée	Admissible	Réduction
4	• 40 % des transactions par des dispositifs à puce • 90 % des emplacements utilisent d'autres technologies d'atténuation des risques	Non	50 % : Réduction standard (moins de 75 % de transactions avec des dispositifs à puce ne permettent pas une admissibilité à la réduction améliorée)

[1] Un incident touchant les données de 10 000 comptes-Cartes American Express à un taux de 5,00 $ 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 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 suspecté :** 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 ou de correction dès le signalement par American Express.
- Vous devez fournir des documents de validation de normes SCP mis à jour conformément à la Section 2, « Programme de conformité aux normes SCP (Importante validation périodique de vos systèmes) ».
- Le cas échéant, vous devez embaucher un enquêteur judiciaire du SCP 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
  - 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 2-7 : 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 appliqués lorsque vos obligations en vertu du Programme d'analyse ciblée ne sont pas satisfaites avant la première échéance.	25 000 $ US	5 000 $ US	1 000 $ US
Des frais de non-conformité peuvent être imposés lorsque vos 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 vos 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 que le Programme d'analyse ciblée soit résolu.*	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 6 Confidentialité

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, 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. EN VERTU DES PRÉSENTES EXIGENCES SUR LA SÉCURITÉ DES DONNÉES, LES ÉMETTEURS DE CARTE AMERICAN EXPRESS NE SONT PAS DES TIERS BÉNÉFICIAIRES.

Section 8 Glossaire

Aux fins de ces *Lignes directrices sur la sécurité des données uniquement*, les définitions suivantes s'appliqueront et prévaudront.

Données de compte désigne les données du titulaire de la Carte et (ou) d'authentification sensibles. Se reporter à Données sur le titulaire et Données d'authentification sensibles.

Convention désigne les dispositions générales, le Règlement des marchands et toutes les annexes ou pièces jointes, collectivement (parfois appelé la Convention d'acceptation de la Carte dans nos documents).

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.

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

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).

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.).

Transactions de paiement par l'acheteur (TPA) désigne une solution de paiement numérique qui permet aux acheteurs de planifier de manière rapide et efficace des paiements à l'intention des fournisseurs (en lien avec les cartes d'entreprise).

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

Données du titulaire de la Carte signifie, au minimum, le numéro de compte primaire (NCP) complet utilisé seul ou le NCP complet accompagné des informations suivantes : nom du titulaire de la carte, date d'expiration et/ou code de service. Se reporter aux 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.

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 d'authentification sensibles.

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.

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).

Émetteur de la Carte 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.

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

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

Reçu d'opération signifie un enregistrement reproductible (à la fois sur papier et sur support électronique) d'une opération qui est conforme à nos exigences et qui contient le numéro de la Carte, la date de la transaction, le montant en dollars, le code d'autorisation, la signature du titulaire (le cas échéant) et d'autres renseignements.

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

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 transactions par Cartes à puce conformes aux spécifications PCPAE.

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

Consommateur désigne un titulaire de la Carte qui achète des biens, des services, 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.

Crédit désigne le montant de l'opération que vous remboursez à un titulaire relativement à un achat ou à un paiement porté à la Carte.

Bordereau de crédit désigne un bordereau de crédit conforme à nos exigences.

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 autorisés 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 ou que vous 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).

Fenêtre de l'incident touchant les données désigne la fenêtre de compromission (ou une période de temps déterminée de manière similaire) indiquée dans le rapport final de l'expert judiciaire (p. ex., le rapport de l'enquête judiciaire du SCP) ou, si elle est inconnue, jusqu'à 365 jours avant la dernière date de notification des

numéros de Cartes potentiellement compromis dans le cadre d'une compromission de données qui nous a été signalée.

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

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 « carte 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 approbations de type EMVCo sont indiquées à l'adresse www.emvco.com.

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

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 https://www.pcisecuritystandards.org.

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 de l'opérateur; 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.

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 moins de 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 moins de 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.

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.

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.

Niveau des marchands désigne le classement des marchands en fonction du respect de leurs obligations en matière de conformité aux normes SCP, telles qu'elles sont énoncées à la Section 2, « Programme de conformité aux normes SCP (Importante validation périodique de vos systèmes) ».

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.

Application de paiement a la signification donnée dans le glossaire en vigueur des termes 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), accessible sur le site www.pcisecuritystandards.org.

Normes de sécurité des données de l'industrie des cartes de paiement (Normes SCP) désigne les normes de sécurité des données 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 et les normes de sécurité des données d'application de paiement (PA DSS), accessibles à 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.

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

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.

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.

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.

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.

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.

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 doivent utiliser le Portail pour présenter les documents de validation de SCP à American Express.

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

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.

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

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.

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.

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.

Questionnaire d'autoévaluation (SAQ) 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.

Données d'authentification sensibles désigne les informations liées à la sécurité, utilisées pour authentifier les titulaires de 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 NIP et les blocs de NIP.

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.

Programme d'analyse ciblée désigne un programme qui fournit une détermination hâtive d'une compromission possible des données du titulaire de Carte dans votre EDTC. Voir la Section 5, « Programme d'analyse ciblée ».

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

Transaction désigne une opération, un crédit, une avance de fonds (ou tout autre accès à des liquidités) ou une transaction à un guichet automatique effectuée au moyen d'une Carte.

Données de transaction désigne tout renseignement exigé par American Express pour documenter une ou plusieurs transactions, y compris les données obtenues ou générées au point de vente durant les étapes d'autorisation et de présentation, et les éventuels débits compensatoires.

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.

Section 9 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

EMVCo : www.emvco.com