AMERICAN EXPRESS

Exigences en matière de sécurité des données

Canada

Octobre 2020

Le présent document a été conçu aux fins d'utilisation par les marchands qui ont conclu une convention légalement exécutoire avec un fournisseur de services aux marchands situé au Canada, en vue de l'acceptation de la Carte American Express[MD].

DON'T do business WITHOUT IT℠

AMERICAN EXPRESS

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. La mise en place de Lignes directrices opérationnelles sur la sécurité peut contribuer à augmenter la confiance des clients et peut améliorer la rentabilité et la réputation d'une entreprise.

American Express sait que les marchands (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 conclue avec votre fournisseur de services aux marchands en ce qui concerne l'acceptation de la Carte American Express[MD] (la Convention) et les présentes exigences en matière de 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 (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.

Section 1 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;
- se conformer aux normes DSP et autres normes SSC (Conseil des normes de sécurité) en vigueur en lien avec la manière dont vous traitez, stockez ou transmettez les données d'un titulaire de la carte ou des données d'authentification sensibles au plus tard à la date d'entrée en vigueur de la mise en œuvre de cette version de la norme de sécurité des données de l'industrie des cartes de paiement; 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 dans des établissements en présence du marchand.

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 ou autrement, de vous assurer de la conformité des tiers visés à l'égard des présentes dispositions sur la sécurité des données (autrement que pour prouver la conformité de vos tiers visés avec ses lignes directrices aux termes de la Section 4 ci-dessous).

Section 2 Obligations en matière de gestion des incidents touchant les données

Vous devez aviser votre fournisseur de services aux marchands immédiatement au moment de la découverte d'un 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, vous devez engager un enquêteur judiciaire du SCP (**PFI**) pour mener cette enquête dans les cinq (5) jours suivant la découverte d'un incident touchant les données.
- Le rapport de vérification judiciaire doit être fourni à votre fournisseur de services aux marchands, *sans modification*, dans le délai prévu par ce dernier.
- Vous devez rapidement fournir à votre fournisseur de services aux marchands la liste des numéros des 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 et vérifier votre capacité 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 de votre fournisseur de services aux marchands, vous devez présenter une validation par un évaluateur de sécurité qualifié (**ÉSQ**) indiquant que ces lacunes ont été corrigées.

Nonobstant les paragraphes précédents de la présente Section 2 :

- American Express peut, à sa seule discrétion, vous demander de faire appel à un PFI 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 2, 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 votre fournisseur de services aux marchands et avec American Express pour corriger tout problème découlant de l'incident, y compris consulter votre fournisseur de services aux marchands au sujet de vos communications avec les titulaires de la Carte touchés par l'incident et fournir à votre fournisseur de services aux marchands (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 de Carte American Express, 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 3 Réservé

Section 4 IMPORTANT! Validation périodique de vos systèmes

Chaque trimestre et chaque année, vous devez effectuer les actions 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) qui servent à stocker, à traiter et à transmettre des clés de chiffrement, des données sur les titulaires de la Carte ou des données d'authentification sensibles (ou une combinaison de ces éléments).

Quatre actions sont nécessaires à la validation :

Action 1 – Participer au programme de conformité d'American Express en vertu des présentes lignes directrices.

Action 2 – Comprendre votre niveau et les documents de validation à fournir.

Action 3 – Remplir les documents de validation que vous devez envoyer à votre fournisseur de services aux marchands.

Action 4 – Faire parvenir les documents de validation à votre fournisseur de services aux marchands dans les délais prescrits.

Action 1 Participer au programme de conformité d'American Express en vertu des présentes lignes directrices

Les marchands de niveaux 1 et 2 et tous les fournisseurs de services décrits ci-dessous doivent participer au programme de conformité SCP d'American Express aux termes des présentes lignes directrices en fournissant le nom complet, l'adresse électronique, le numéro de téléphone et l'adresse postale physique de la personne qui agit à titre de personne-ressource en matière de sécurité des données. Vous devez soumettre ces informations à votre fournisseur de services aux marchands. Vous devez informer votre fournisseur de services aux marchands si ces informations changent, en lui transmettant les renseignements à jour, le cas échéant. Le défaut de fournir ces coordonnées peut entraîner l'imposition de frais de non-conformité. Veuillez communiquer avec votre fournisseur de services aux marchands pour obtenir davantage de renseignements concernant ses exigences de conformité en matière de sécurité des données.

À sa seule discrétion, American Express peut exiger de la part de certains marchands de niveau 3 et de niveau 4 qu'ils participent au programme de conformité d'American Express aux termes des présentes lignes directrices en leur envoyant un avis écrit à cet effet. Ces marchands doivent s'inscrire au programme de conformité au plus tard 90 jours après la réception de l'avis.

Action 2 Comprendre votre niveau et les documents de validation à fournir

Les niveaux des marchands sont établis en fonction du volume de transactions que vous portez à la Carte American Express. Pour les marchands, il s'agit du volume présenté par leurs établissements. Vous serez classé dans l'un des niveaux décrits ci-dessous.

Exigences pour les marchands

Il existe quatre (4) classements possibles pour les marchands en ce qui concerne leur niveau et les documents de validation qu'ils doivent fournir. Après avoir déterminé le niveau de marchand dans la liste ci-dessous, consultez le tableau des marchands 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 désigne, 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 – De 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.

Niveau de marchand/ Transactions American Express annuelles	Documents de validation		
	Rapport d'évaluation de conformité sur place	Questionnaire d'autoévaluation (QAÉ) et exercice trimestriel de balayage du réseau	Attestation du PATS pour les marchands admissibles
Niveau 1/ 2,5 millions ou plus	Obligatoire	Sans objet	Facultatif (remplace le Rapport d'évaluation de conformité sur place)
Niveau 2/ 50 000 à 2,5 millions	Facultatif	QAÉ obligatoire (sauf si l'on soumet un rapport de vérification annuelle de la sécurité sur les lieux); balayage obligatoire avec certains types de QAÉ	Facultatif (remplace le QAÉ et le balayage du réseau ou le Rapport d'évaluation de conformité sur place)
Niveau 3*/ 10 000 à 50 000	Facultatif	QAÉ facultatif (obligatoire si exigé par American Express); balayage obligatoire avec certains types de QAÉ	Facultatif (remplace le QAÉ et le balayage du réseau ou le Rapport d'évaluation de conformité sur place)
Niveau 4*/ 10 000 ou moins	Facultatif	QAÉ facultatif (obligatoire si exigé par American Express); balayage obligatoire avec certains types de QAÉ	Facultatif (remplace le QAÉ 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 présentes exigences en matière de sécurité des données et s'acquitter de leurs responsabilités en vertu de celles-ci.

American Express se réserve le droit de vérifier l'exactitude et le caractère approprié de la documentation de validation PCI en engageant, aux frais d'American Express, un ÉSQ ou PFI de notre choix.

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. Le PATS s'applique uniquement si le marchand n'a pas enregistré d'incident touchant les données au cours des 12 derniers mois et si 75 % de toutes les transactions par Carte du marchand sont traitées en utilisant :

- **La technologie EMV** – sur un dispositif à puce actif avec une approbation/attestation EMVCo valide et à jour (www.emvco.com) et pouvant traiter des transactions par Cartes à puce conformes aux spécifications PCPAE.
- **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.

  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 l'Action 3 ci-dessous.

Action 3 Remplir les documents de validation que vous devez envoyer à votre fournisseur de services aux marchands

Les documents ci-dessous sont requis pour les différents niveaux de marchand énumérés dans le tableau ci-dessus.

Vérification annuelle de la sécurité sur les lieux – La vérification annuelle de la sécurité sur les lieux est un examen détaillé de votre matériel, de vos systèmes et de vos réseaux (et de leurs composantes) où les clés de chiffrements, les données sur les titulaires de la Carte ou les données d'authentification sensibles (ou une combinaison de ces éléments) sont conservées, traitées ou transmises. La vérification doit être effectuée par :

- un ÉSQ; ou
- vous et doit être attestée par votre chef de la direction, votre directeur financier, votre chef de la sécurité de l'information ou votre mandant et doit être soumise à votre fournisseur de services aux marchands chaque année, accompagnée de l'attestation de conformité applicable (**AOC**).

Cette dernière doit appuyer la conformité à toutes les exigences des normes SCP et, sur demande, inclure une copie de l'intégralité du rapport de conformité (marchands de niveau 1).

Questionnaire d'autoévaluation annuelle – L'autoévaluation annuelle est un processus où vous utilisez le questionnaire d'autoévaluation (**QAÉ**) fourni avec les normes SCP pour vérifier la conformité de vos systèmes, de votre matériel et de vos réseaux (et leurs composantes) où les clés de chiffrement, les données sur les titulaires de la Carte ou les données d'authentification sensibles (ou une combinaison de ces éléments) sont conservées, traitées ou transmises. Vous devez le remplir et le faire certifier par votre chef de la direction, votre directeur financier, votre chef de la sécurité de l'information ou votre mandant. La section du questionnaire d'autoévaluation portant sur l'attestation de conformité doit être soumise chaque année à votre fournisseur de services aux marchands. La section de l'attestation de conformité du QAÉ doit certifier votre conformité à toutes les exigences des normes SCP et inclure des copies intégrales du QAÉ sur demande (les marchands de niveau 2, de niveau 3 et de niveau 4).

Exercice trimestriel de balayage du réseau – L'exercice trimestriel de balayage du réseau sert à vérifier à distance si votre réseau informatique et vos serveurs Web reliés à Internet sont vulnérables ou s'ils présentent des faiblesses. Il doit être exécuté par un fournisseur de services de balayage autorisé (**FSBA**). Vous devez remplir l'attestation de conformité par balayage du FSBA (**AOSC**) ou le sommaire des résultats du balayage (et des copies du balayage complet, sur demande) et les soumettre chaque trimestre à votre fournisseur de services aux marchands. L'attestation de conformité par balayage ou le sommaire des résultats doivent attester que les résultats du balayage sont conformes aux processus de balayage de la norme SCP, qu'aucun problème de sécurité majeur n'a été décelé et que le balayage a eu lieu ou qu'il est conforme (tous les marchands, à l'exception de ceux qui soumettent également un Rapport de vérification annuelle de la sécurité sur les lieux et de ceux admissibles au PATS). Pour éviter toute confusion, les exercices trimestriels de balayage du réseau sont obligatoires s'ils sont exigés par le questionnaire d'autoévaluation applicable.

Documents de validation de l'attestation annuelle du PATS – L'Attestation annuelle du PATS d'American Express (**« l'Attestation PATS »**) est uniquement disponible pour les marchands qui satisfont aux critères mentionnés à l'Action 2 ci-dessus. L'Attestation PATS est un processus utilisant les normes SCP du PCI qui permet l'auto-examen de votre matériel, de vos systèmes et de vos réseaux (et de leurs composantes) sur lesquels les clés de chiffrement, les données sur les titulaires ou les données d'authentification sensibles (ou une combinaison de ces éléments) sont conservées, traitées ou transmises. Vous devez le remplir et le faire certifier par votre chef de la direction, votre directeur financier, votre chef de la sécurité de l'information ou votre mandant. Vous devez terminer le processus en soumettant chaque année le formulaire d'Attestation PATS à votre fournisseur de services aux marchands. (Marchands admissibles au PATS seulement.)

Rapport de conformité – Le rapport de conformité (**SOC**) est un document par lequel un franchiseur ou un fournisseur de services peut signaler le statut de conformité SCP de ses franchisés. Le modèle du rapport de conformité est disponible en téléchargement via le portail sécurisé de SecureTrust.

Non-conformité aux normes SCP – Si vous ne vous conformez pas aux normes SCP, vous devez soumettre un des documents suivants :

- une Attestation de conformité (AOC) comprenant la « Partie 4. Plan d'action pour le statut de non-conformité »
- un sommaire d'approche prioritaire et attestation de conformité aux normes SCP (PASAOC)
- un modèle de plan de projet (disponible auprès de votre fournisseur de services aux marchands)

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 présenter les documents appropriés à votre fournisseur de services aux marchands. Vous devez régulièrement faire un suivi auprès de votre fournisseur de services aux marchands relativement à votre progrès en ce qui a trait à la correction de votre statut de non-conformité (marchands de niveaux 1, 2, 3 et 4). Pour éviter toute confusion, les marchands qui ne respectent pas les normes SCP ne sont pas admissibles au PATS.

Action 4 Faire parvenir les documents de validation à votre fournisseur de services aux marchands

Tous les marchands qui doivent participer au programme de conformité SCP d'American Express doivent soumettre les documents de validation portant la mention « Obligatoire », comme il est indiqué au tableau de l'Action 2.

Vous devez présenter vos documents de validation à votre fournisseur de services aux marchands. Si vous avez des questions d'ordre général sur le programme ou le processus ci-dessus, veuillez communiquer avec votre fournisseur de services aux marchands.

La validation et les mesures à prendre en matière de conformité sont à vos frais. En envoyant vos documents de validation à votre fournisseur de services aux marchands, vous déclarez et garantissez que vous êtes autorisé à divulguer les renseignements qu'ils contiennent à votre fournisseur de services aux marchands et à American Express, et que vous transmettez les documents de validation sans violer les droits d'une autre partie.

Frais de non-validation et résiliation de la Convention

American Express et votre fournisseur de services aux marchands ont le droit de vous imposer des frais pour non-validation et de résilier la Convention si vous ne répondez pas aux présentes exigences ou si vous ne transmettez pas les documents de validation exigés dans les délais prescrits. Votre fournisseur de services aux marchands vous informera de l'échéance à respecter pour chaque période de déclaration annuelle et trimestrielle.

Si votre fournisseur de services aux marchands ne reçoit pas vos documents de validation obligatoires du marchand, votre fournisseur de services aux marchands a le droit de résilier la Convention, conformément aux modalités qui y sont énoncées, et de vous imposer des frais de non-validation.

Section 5 Réservé

Section 6 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 DES ÉSQ, DES FSBA OU DES PFI (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

Exigences en matière de sécurité des données d'American Express :

www.americanexpress.ca/esd

PCI Security Standards Council, LLC :

www.pcisecuritystandards.org

Glossaire

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

Application de paiement

A le sens défini dans le glossaire alors en vigueur des normes de sécurité des données d'application de paiement du SCP, que vous trouverez à l'adresse www.pcisecuritystandards.org.

Approuvé par le secteur des cartes de paiement

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 par balayage, ou AOSC

Une 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.).

Attestation de conformité, ou AOC

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 des normes de sécurité des données du secteur des cartes de paiement, s.r.l.).

Carte American Express ou Carte

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

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 », « carte ICC » ou « carte à puce intégrée » ou dans nos documents).

Chiffrement point à point (P2PE)

Une solution de protection cryptographique des données d'un compte qui s'étend du point où le marchand accepte la carte de paiement jusqu'au point de déchiffrement sécuritaire.

Clé de chiffrement (« clé de chiffrement American Express »)

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 ZPK

Crédit

Le montant que vous remboursez à un titulaire relativement à un achat ou à un paiement porté à la Carte.

Date de signalement

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

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.

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.

Documents de validation

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 le sens défini dans le glossaire alors en vigueur des normes SCP.

Données sur le titulaire

A le sens défini dans le glossaire alors en vigueur des normes SCP.

Enquêteur judiciaire du SCP ou PFI

Une entité qui a été approuvée par le conseil sur les normes de sécurité du secteur des cartes de paiement, une personne morale à responsabilité limitée, en vue de procéder à la vérification judiciaire d'une fuite ou d'une compromission des données sur la carte de paiement.

Exigences du Conseil des normes de sécurité de l'industrie des cartes de paiement (Payment Card Industry Security Standards Council, ou normes SCP)

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, qui est disponible à www.pcisecuritystandards.org.

Exigences relatives à la sécurité des transactions avec NIP du SCP

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

Évaluateur de sécurité qualifié ou ÉSQ

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

La période qui commence à la date de la compromission, si elle est connue, ou 365 jours avant la date de signalement si la date exacte de la compromission est inconnue. La fenêtre de l'incident touchant les données se termine 30 jours après la date de signalement.

Fournisseur de services

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 aux marchands

La société de traitement de la carte utilisée pour le paiement du marchand ou toute entité auprès de laquelle le marchand reçoit des services de traitement. Ces services peuvent comprendre, entre autres, le traitement des transactions, la facilitation des autorisations relatives aux achats et de la saisie de données, la comptabilité des marchands, les opérations d'arrière-guichet (p. ex. débits compensatoires et détection de la fraude), la prestation de matériel au point de vente, les solutions, les systèmes, les ventes ou le service à la clientèle.

Fournisseurs de services de balayage autorisés ou FSBA

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, au moyen d'évaluations de la vulnérabilité des systèmes électroniques (sur Internet).

Franchiseur

L'exploitant d'une entreprise qui accorde à des personnes ou à des entités (franchisés) une licence pour distribuer des biens (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.

Franchisé

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.

Incident touchant les données

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;
- 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 chiffrements, les données sur les titulaires ou les données d'authentification sensibles (ou une combinaison de ces éléments).

Marchand

Le marchand et toutes ses sociétés affiliées qui ont conclu une convention légalement exécutoire avec un fournisseur de services aux marchands situé au Canada, en vue de l'acceptation de la Carte American Express[MD].

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 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

De 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.

Modèle de rapport d'enquête final

Le modèle fourni par le conseil des normes de sécurité du SCP, disponible au www.pcisecuritystandards.org.

Normes SCP

Les normes de sécurité des données du secteur des cartes de paiement, accessibles à l'adresse https://www.pcisecuritystandards.org.

Numéro de Carte

Le numéro d'identification unique que l'émetteur attribue à une Carte au moment où elle est émise.

Numéro de Carte compromis

Un numéro de compte-Carte American Express associé à un incident touchant les données.

Opération

Un paiement ou un achat porté à une Carte.

Programme d'amélioration des technologies de sécurité (PATS)

Le programme d'American Express dans le cadre duquel les marchands sont encouragés à déployer des technologies qui renforcent la sécurité des données. Pour être admissibles au PATS, les marchands doivent n'avoir connu aucun incident concernant les données au cours des 12 mois précédant l'attestation de conformité annuelle, et doivent avoir traité au moins 75 % de toutes leurs transactions en utilisant le chiffrement point à point, ou encore à l'aide de dispositifs à puce actifs de norme EMV, devant une carte présentée physiquement par le titulaire.

Puce

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

Questionnaire d'autoévaluation ou QAÉ

Un outil d'autoévaluation conçu 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 d'évaluer et d'attester la conformité aux normes SCP.

Rapport de conformité ou SOC

Un document de validation SCP utilisé par un franchiseur pour indiquer le statut de conformité aux normes SCP de ses franchisés concernés.

Société de traitement

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

Toute solution figurant sur la liste des solutions validées selon les normes SCP ou validée par un évaluateur de sécurité qualifié P2PE approuvé par les normes SCP.

Spécifications EMV

Les spécifications émises par EMVCo, LLC qui sont disponibles à www.emvco.com.

Terminal point de vente (PdV)

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 une transaction, ou les deux.

Titulaire de la Carte

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.

Tiers visés

L'ensemble de vos employés, agents, représentants, sous-traitants, sociétés de traitement, fournisseurs de services ou fournisseurs de matériel ou de terminaux point de vente (PdV) ou de solutions de traitement des paiements, entités associées à votre compte de marchand American Express et toute autre partie à laquelle vous donnez un accès aux données sur les titulaires ou aux données d'authentification sensibles (ou aux deux) conformément à la Convention.

Transaction

Un paiement ou crédit réalisé au moyen de la Carte.

Transaction par EMV

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'EMV valide et à jour. Les types d'approbations d'EMV sont indiqués à l'adresse http://www.emvco.com.

Vérification de l'état du compte

Un type de demande d'autorisation qui est utilisé pour demander à un émetteur d'indiquer si le compte de carte représenté par le numéro de carte sur le message est valide. Le contrôle de l'état des comptes est utilisé, par exemple, par les autorités de transit pour vérifier l'état d'un compte de carte associé à une transaction de transit sans contact au terminal de l'opérateur de transit.

AMERICAN EXPRESS

Exigences en matière de sécurité des données

Canada

Octobre 2020

Le présent document a été conçu aux fins d'utilisation par les marchands qui ont conclu une convention légalement exécutoire avec un fournisseur de services aux marchands situé au Canada, en vue de l'acceptation de la Carte American Express[MD].

DON'T do business WITHOUT IT℠

AMERICAN EXPRESS

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. La mise en place de Lignes directrices opérationnelles sur la sécurité peut contribuer à augmenter la confiance des clients et peut améliorer la rentabilité et la réputation d'une entreprise.

American Express sait que les marchands (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 conclue avec votre fournisseur de services aux marchands en ce qui concerne l'acceptation de la Carte American Express[MD] (la Convention) et les présentes exigences en matière de 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 (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.

Section 1 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;
- se conformer aux normes DSP et autres normes SSC (Conseil des normes de sécurité) en vigueur en lien avec la manière dont vous traitez, stockez ou transmettez les données d'un titulaire de la carte ou des données d'authentification sensibles ~~dans le secteur des cartes de paiement (normes SCP)~~ au plus tard à la date d'entrée en vigueur de la mise en œuvre de cette version de la norme de sécurité des données de l'industrie des cartes de paiement; 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 dans des établissements en présence du marchand.

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 ou autrement, de vous assurer de la conformité des tiers visés à l'égard des présentes dispositions sur la sécurité des données (autrement que pour prouver la conformité de vos tiers visés avec ses lignes directrices aux termes de la Section 4 ci-dessous).

Section 2 Obligations en matière de gestion des incidents touchant les données

Vous devez aviser votre fournisseur de services aux marchands immédiatement au moment de la découverte d'un 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, vous devez engager un enquêteur judiciaire du SCP (**PFI**) pour mener cette enquête dans les cinq (5) jours suivant la découverte d'un incident touchant les données.
- Le rapport de vérification judiciaire doit être fourni à votre fournisseur de services aux marchands, *sans modification*, dans le délai prévu par ce dernier.
- Vous devez rapidement fournir à votre fournisseur de services aux marchands la liste des numéros des 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 et vérifier votre capacité ~~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 ~~confirmant votre participation~~ au programme de conformité d'American Express (comme décrit ci-dessous). À la demande de votre fournisseur de services aux marchands, vous devez présenter une validation par un évaluateur de sécurité qualifié (**ÉSQ**) indiquant que ces lacunes ont été corrigées.

Nonobstant les paragraphes précédents de la présente Section 2 :

- American Express peut, à sa seule discrétion, vous demander de faire appel à un PFI 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 2, 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 votre fournisseur de services aux marchands et avec American Express pour corriger tout problème découlant de l'incident, y compris consulter votre fournisseur de services aux marchands au sujet de vos communications avec les titulaires de la Carte touchés par l'incident et fournir à votre fournisseur de services aux marchands (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 de Carte American Express, 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 3 Réservé

Section 4 IMPORTANT! Validation périodique de vos systèmes

Chaque trimestre et chaque année, vous devez effectuer les actions ~~étapes~~ 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) qui servent à stocker, à traiter et à transmettre des clés de chiffrement, des données sur les titulaires de la Carte ou des données d'authentification sensibles (ou une combinaison de ces éléments).

Quatre actions ~~étapes~~ sont nécessaires à la validation :

Action ~~Étape~~ 1 – Participer au programme de conformité d'American Express en vertu des présentes lignes directrices.

Action ~~Étape~~ 2 – Comprendre votre niveau et les documents de validation à fournir.

Action ~~Étape~~ 3 – Remplir les documents de validation que vous devez envoyer à votre fournisseur de services aux marchands.

Action ~~Étape~~ 4 – Faire parvenir les documents de validation à votre fournisseur de services aux marchands dans les délais prescrits.

Action 1 Participer au programme de conformité d'American Express en vertu des présentes lignes directrices

Les marchands de niveaux 1 et 2 et tous les fournisseurs de services décrits ci-dessous doivent participer au programme de conformité SCP d'American Express ~~programme de conformité d'American Express~~ aux termes des présentes lignes directrices en fournissant le nom complet, l'adresse électronique, le numéro de téléphone et l'adresse postale physique de la personne qui agit à titre de personne-ressource en matière de sécurité des données. Vous devez soumettre ces informations à votre fournisseur de services aux marchands. Vous devez informer votre fournisseur de services aux marchands si ces informations changent, en lui transmettant les renseignements à jour, le cas échéant. Le défaut de fournir ces coordonnées peut entraîner l'imposition de frais de non-conformité. ~~soumettre les documents de validation périodiques applicables à votre fournisseur de~~

~~services aux marchands.~~ Veuillez communiquer avec votre fournisseur de services aux marchands pour obtenir davantage de renseignements concernant ses exigences de conformité en matière de sécurité des données.

À sa seule discrétion, American Express peut exiger de la part de certains marchands de niveau 3 et de niveau 4 qu'ils participent au programme de conformité d'American Express aux termes des présentes lignes directrices en leur envoyant un avis écrit à cet effet. Ces marchands doivent s'inscrire au programme de conformité au plus tard 90 jours après la réception de l'avis.

~~À sa seule discrétion, American Express peut exiger de la part de certains marchands de niveau 3 et de niveau 4 qu'ils participent au programme de conformité d'American Express aux termes des présentes lignes directrices. Un avis écrit à cet effet sera envoyé à votre fournisseur de services aux marchands. Ces marchands doivent s'inscrire au programme de conformité au plus tard 90 jours après la réception de l'avis.~~

~~American Express se réserve le droit de vérifier les résultats de votre processus de validation en fonction des normes SCP, notamment en engageant, aux frais d'American Express, un ÉSQ de son choix.~~

Action 2 Comprendre votre niveau et les documents de validation à fournir

Les niveaux des marchands sont établis en fonction du volume de transactions que vous portez à la Carte American Express. Pour les marchands, il s'agit du volume présenté par leurs établissements. Vous serez classé dans l'un des niveaux décrits ci-dessous.

Exigences pour les marchands

Il existe quatre (4) classements possibles pour les marchands en ce qui concerne leur niveau et les documents de validation qu'ils doivent fournir. Après avoir déterminé le niveau de marchand dans la liste ci-dessous, consultez le tableau des marchands 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 désigne~~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 – De 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.

Niveau de marchand/ Transactions American Express annuelles	Documents de validation		
	Rapport d'évaluation de conformité sur place	Questionnaire d'autoévaluation (QAÉ) et exercice trimestriel de balayage du réseau	Attestation du PATS pour les marchands admissibles
Niveau 1/ 2,5 millions ou plus	Obligatoire	Sans objet	Facultatif (remplace le Rapport d'évaluation de conformité sur place)
Niveau 2/ 50 000 à 2,5 millions	Facultatif	QAÉ obligatoire (sauf si l'on soumet un rapport de vérification annuelle de la sécurité sur les lieux); balayage obligatoire avec certains types de QAÉ	Facultatif (remplace le QAÉ et le balayage du réseau ou le Rapport d'évaluation de conformité sur place)

Niveau de marchand/ Transactions American Express annuelles	Documents de validation		
	Rapport d'évaluation de conformité sur place	Questionnaire d'autoévaluation (QAÉ) et exercice trimestriel de balayage du réseau	Attestation du PATS pour les marchands admissibles
Niveau 3*/ 10 000 à 50 000	Facultatif	QAÉ facultatif (obligatoire si exigé par American Express); balayage obligatoire avec certains types de QAÉ	Facultatif (remplace le QAÉ et le balayage du réseau ou le Rapport d'évaluation de conformité sur place)
Niveau 4*/ 10 000 ou moins	Facultatif	QAÉ facultatif (obligatoire si exigé par American Express); balayage obligatoire avec certains types de QAÉ	Facultatif (remplace le QAÉ 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 présentes exigences en matière de sécurité des données et s'acquitter de leurs responsabilités en vertu de celles-ci.

American Express se réserve le droit de vérifier l'exactitude et le caractère approprié de la documentation de validation PCI en engageant, aux frais d'American Express, un ÉSQ ou PFI de notre choix.

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. Le PATS s'applique uniquement si le marchand n'a pas enregistré d'incident touchant les données au cours des 12 derniers mois et si 75 % de toutes les transactions par Carte du marchand sont traitées en utilisant :

- **La technologie EMV** – sur un dispositif à puce actif avec une approbation/attestation EMVCo valide et à jour (www.emvco.com) et pouvant traiter des transactions par Cartes à puce conformes aux spécifications PCPAE.
- **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.

  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 l'Action 3 ci-dessous.

Action 3 Remplir les documents de validation que vous devez envoyer à votre fournisseur de services aux marchands

Les documents ci-dessous sont requis pour les différents niveaux de marchand énumérés dans le tableau ci-dessus.

Vérification annuelle de la sécurité sur les lieux – La vérification annuelle de la sécurité sur les lieux est un examen détaillé de votre matériel, de vos systèmes et de vos réseaux (et de leurs composantes) où les clés de chiffrements, les données sur les titulaires de la Carte ou les données d'authentification sensibles (ou une combinaison de ces éléments) sont conservées, traitées ou transmises. La vérification doit être effectuée par :

- un ÉSQ; ou
- vous et doit être attestée ~~certifiée~~ par votre chef de la direction, votre directeur financier, votre chef de la sécurité de l'information ou votre mandant et doit être soumise à votre fournisseur de services aux marchands chaque année, accompagnée de l'attestation de conformité applicable (**AOC**).

Cette dernière doit appuyer ~~certifier~~ la conformité à toutes les exigences des normes SCP et, sur demande, inclure une copie de l'intégralité du rapport de conformité (marchands de niveau 1).

Questionnaire d'autoévaluation annuelle – L'autoévaluation annuelle est un processus où vous utilisez le questionnaire d'autoévaluation (**QAÉ**) fourni avec les normes SCP pour vérifier la conformité de vos systèmes, de votre matériel et de vos réseaux (et leurs composantes) où les clés de chiffrement, les données sur les titulaires de la Carte ou les données d'authentification sensibles (ou une combinaison de ces éléments) sont conservées, traitées ou transmises. Vous devez le remplir et le faire certifier par votre chef de la direction, votre directeur financier, votre chef de la sécurité de l'information ou votre mandant. La section du questionnaire d'autoévaluation portant sur l'attestation de conformité doit être soumise chaque année à votre fournisseur de services aux marchands. La section de l'attestation de conformité du QAÉ doit certifier votre conformité à toutes les exigences des normes SCP et inclure des copies intégrales du QAÉ sur demande (les marchands de niveau 2, de niveau 3 et de niveau 4).

Exercice trimestriel de balayage du réseau – L'exercice trimestriel de balayage du réseau sert à vérifier à distance si votre réseau informatique et vos serveurs Web reliés à Internet sont vulnérables ou s'ils présentent des faiblesses. Il doit être exécuté par un fournisseur de services de balayage autorisé (**FSBA**). Vous~~Chaque trimestre, vous~~ devez remplir l'attestation de conformité par balayage du FSBA (**AOSC**) ou le sommaire des résultats du balayage (et des copies du balayage complet, sur demande) et les soumettre chaque trimestre à votre fournisseur de services aux marchands. L'attestation de conformité par balayage ou le sommaire des résultats doivent attester que les résultats du balayage sont conformes aux processus de balayage de la norme SCP, qu'aucun problème de sécurité majeur n'a été décelé et que le balayage a eu lieu ou qu'il est conforme (tous les marchands, à l'exception de ceux qui soumettent également un Rapport de vérification annuelle de la sécurité sur les lieux et de ceux admissibles au PATS). Pour éviter toute confusion, les exercices trimestriels de balayage du réseau sont obligatoires s'ils sont exigés par le questionnaire d'autoévaluation applicable.

Documents de validation de l'attestation annuelle du PATS – L'Attestation annuelle du PATS d'American Express (**« l'Attestation PATS »**) est uniquement disponible pour les marchands qui satisfont aux critères mentionnés à l'Action 2 ci-dessus. L'Attestation PATS est un processus utilisant les normes SCP du PCI qui permet l'auto-examen de votre matériel, de vos systèmes et de vos réseaux (et de leurs composantes) sur lesquels les clés de chiffrement, les données sur les titulaires ou les données d'authentification sensibles (ou une combinaison de ces éléments) sont conservées, traitées ou transmises. Vous devez le remplir et le faire certifier par votre chef de la direction, votre directeur financier, votre chef de la sécurité de l'information ou votre mandant. Vous devez terminer le processus en soumettant chaque année le formulaire d'Attestation PATS à votre fournisseur de services aux marchands. (Marchands admissibles au PATS seulement.)

Rapport de conformité – Le rapport de conformité (**SOC**) est un document par lequel un franchiseur ou un fournisseur de services peut signaler le statut de conformité SCP de ses franchisés. Le modèle du rapport de conformité est disponible en téléchargement via le portail sécurisé de SecureTrust.

Non-conformité aux normes SCP – Si vous ne vous conformez pas aux normes SCP, vous devez soumettre un des documents suivants :

- une Attestation de conformité (AOC) comprenant la « Partie 4. Plan d'action pour le statut de non-conformité »
- un sommaire d'approche prioritaire et attestation de conformité aux normes SCP (PASAOC)
- un modèle de plan de projet (disponible auprès de votre fournisseur de services aux marchands)

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 présenter les documents appropriés à votre fournisseur de services aux marchands. Vous devez régulièrement faire un suivi auprès de votre fournisseur de services aux marchands relativement à votre progrès en ce qui a trait à la correction de votre statut de non-conformité (marchands de niveaux 1, 2, 3 et 4). Pour éviter toute confusion, les marchands qui ne respectent pas les normes SCP ne sont pas admissibles au PATS.

Action 4 Faire parvenir les documents de validation à votre fournisseur de services aux marchands

Tous les marchands qui doivent participer au programme de conformité SCP d'American Express doivent soumettre les documents de validation portant la mention « Obligatoire », comme il est indiqué au tableau de l'Action 2.

Vous devez présenter vos documents de validation à votre fournisseur de services aux marchands. Si vous avez des questions d'ordre général sur le programme ou le processus ci-dessus, veuillez communiquer avec votre fournisseur de services aux marchands.

La validation et les mesures à prendre en matière de conformité sont à vos frais. En envoyant vos documents de validation à votre fournisseur de services aux marchands, vous déclarez et garantissez que vous êtes autorisé à divulguer les renseignements qu'ils contiennent à votre fournisseur de services aux marchands et à American Express, et que vous transmettez les documents de validation sans violer les droits d'une autre partie.

Frais de non-validation et résiliation de la Convention

American Express et votre fournisseur de services aux marchands ont le droit de vous imposer des frais pour non-validation et de résilier la Convention si vous ne répondez pas aux présentes exigences ou si vous ne transmettez pas les documents de validation exigés dans les délais prescrits. Votre fournisseur de services aux marchands vous informera de l'échéance à respecter pour chaque période de déclaration annuelle et trimestrielle.

Si votre fournisseur de services aux marchands ne reçoit pas vos documents de validation obligatoires du marchand, votre fournisseur de services aux marchands a le droit de résilier la Convention, conformément aux modalités qui y sont énoncées, et de vous imposer des frais de non-validation.

Section 5 Réservé

Section 6 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 DES ÉSQ, DES FSBA OU DES PFI (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

Exigences en matière de sécurité des données d'American Express :

www.americanexpress.ca/esd

PCI Security Standards Council, LLC :

www.pcisecuritystandards.org

Glossaire

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

Application de paiement

A le sens défini dans le glossaire alors en vigueur des normes de sécurité des données d'application de paiement du SCP, que vous trouverez à l'adresse www.pcisecuritystandards.org.

Approuvé par le secteur des cartes de paiement

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 par balayage, ou AOSC

Une 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.).

Attestation de conformité, ou AOC

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 des normes de sécurité des données du secteur des cartes de paiement, s.r.l.).

Carte American Express ou Carte

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

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 », « carte ICC » ou « carte à puce intégrée » ou dans nos documents).

Chiffrement point à point (P2PE)

Une solution de protection cryptographique des données d'un compte qui s'étend du point où le marchand accepte la carte de paiement jusqu'au point de déchiffrement sécuritaire.

Clé de chiffrement (« clé de chiffrement American Express »)

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 ZPK

Crédit

Le montant que vous remboursez à un titulaire relativement à un achat ou à un paiement porté à la Carte.

Date de signalement

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

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.

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.

Documents de validation

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 le sens défini dans le glossaire alors en vigueur des normes SCP.

Données sur le titulaire

A le sens défini dans le glossaire alors en vigueur des normes SCP.

Enquêteur judiciaire du SCP ou PFI

Une entité qui a été approuvée par le conseil sur les normes de sécurité du secteur des cartes de paiement, une personne morale à responsabilité limitée, en vue de procéder à la vérification judiciaire d'une fuite ou d'une compromission des données sur la carte de paiement.

Exigences du Conseil des normes de sécurité de l'industrie des cartes de paiement (Payment Card Industry Security Standards Council, ou normes SCP)

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, qui est disponible à www.pcisecuritystandards.org.

Exigences relatives à la sécurité des transactions avec NIP du SCP

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

Évaluateur de sécurité qualifié ou ÉSQ

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

La période qui commence à la date de la compromission, si elle est connue, ou 365 jours avant la date de signalement si la date exacte de la compromission est inconnue. La fenêtre de l'incident touchant les données se termine 30 jours après la date de signalement.

Fournisseur de services

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 aux marchands

La société de traitement de la carte utilisée pour le paiement du marchand ou toute entité auprès de laquelle le marchand reçoit des services de traitement. Ces services peuvent comprendre, entre autres, le traitement des transactions, la facilitation des autorisations relatives aux achats et de la saisie de données, la comptabilité des marchands, les opérations d'arrière-guichet (p. ex. débits compensatoires et détection de la fraude), la prestation de matériel au point de vente, les solutions, les systèmes, les ventes ou le service à la clientèle.

Fournisseurs de services de balayage autorisés ou FSBA

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, au moyen d'évaluations de la vulnérabilité des systèmes électroniques (sur Internet).

Franchiseur

L'exploitant d'une entreprise qui accorde à des personnes ou à des entités (franchisés) une licence pour distribuer des biens (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.

Franchisé

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.

Incident touchant les données

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;
- 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 chiffrements, les données sur les titulaires ou les données d'authentification sensibles (ou une combinaison de ces éléments).

Marchand

Le marchand et toutes ses sociétés affiliées qui ont conclu une convention légalement exécutoire avec un fournisseur de services aux marchands situé au Canada, en vue de l'acceptation de la Carte American Express[MD].

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 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

De 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.

Modèle de rapport d'enquête final

Le modèle fourni par le conseil des normes de sécurité du SCP, disponible au www.pcisecuritystandards.org.

Normes SCP
Les normes de sécurité des données du secteur des cartes de paiement, accessibles à l'adresse https://www.pcisecuritystandards.org.

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

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

Opération
Un paiement ou un achat porté à une Carte.

Programme d'amélioration des technologies de sécurité (PATS)
Le programme d'American Express dans le cadre duquel les marchands sont encouragés à déployer des technologies qui renforcent la sécurité des données. Pour être admissibles au PATS, les marchands doivent n'avoir connu aucun incident concernant les données au cours des 12 mois précédant l'attestation de conformité annuelle, et doivent avoir traité au moins 75 % de toutes leurs transactions en utilisant le chiffrement point à point, ou encore à l'aide de dispositifs à puce actifs de norme EMV, devant une carte présentée physiquement par le titulaire.

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

Questionnaire d'autoévaluation ou QAÉ
Un outil d'autoévaluation conçu 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 d'évaluer et d'attester la conformité aux normes SCP.

Rapport de conformité ou SOC
Un document de validation SCP utilisé par un franchiseur pour indiquer le statut de conformité aux normes SCP de ses franchisés concernés.

Société de traitement
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
Toute solution figurant sur la liste des solutions validées selon les normes SCP ou validée par un évaluateur de sécurité qualifié P2PE approuvé par les normes SCP.

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

Terminal point de vente (PdV)
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 une transaction, ou les deux.

Titulaire de la Carte

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.

Tiers visés

L'ensemble de vos employés, agents, représentants, sous-traitants, sociétés de traitement, fournisseurs de services ou fournisseurs de matériel ou de terminaux point de vente (PdV) ou de solutions de traitement des paiements, entités associées à votre compte de marchand American Express et toute autre partie à laquelle vous donnez un accès aux données sur les titulaires ou aux données d'authentification sensibles (ou aux deux) conformément à la Convention.

Transaction

Un paiement ou crédit réalisé au moyen de la Carte.

Transaction par EMV

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'EMV valide et à jour. Les types d'approbations d'EMV sont indiqués à l'adresse http://www.emvco.com.

Vérification de l'état du compte

Un type de demande d'autorisation qui est utilisé pour demander à un émetteur d'indiquer si le compte de carte représenté par le numéro de carte sur le message est valide. Le contrôle de l'état des comptes est utilisé, par exemple, par les autorités de transit pour vérifier l'état d'un compte de carte associé à une transaction de transit sans contact au terminal de l'opérateur de transit.