Payment Card Industry (PCI)

Norme de sécurité des données

Attestation de conformité des évaluations sur site – Commerçants

Version 3.2.1

Juin 2018

Section 1 : Informations relatives à l'évaluation

Instructions de transmission

Cette attestation de conformité doit être complétée comme déclaration des résultats de l'auto-évaluation du commerçant vis-à-vis des *Conditions et procédures d'évaluation de sécurité de la norme de sécurité des données du secteur des cartes de paiement (PCI DSS).* Complétez toutes les sections : Le commerçant est responsable de s'assurer que chaque section est remplie par les parties pertinentes, le cas échéant. Contacter votre acquéreur (la banque du commerçant) ou la marque de paiement pour déterminer les procédures de rapport et de demande.

Partie 1. Informations sur l'évaluateur de sécurité qualifié et le commerçant					
Partie 1a. Informations sur le commerçant					
Nom de la société :			DBA (nom commercial) :		
Nom du contact :			Poste occupé :		
Téléphone :			E-mail :		
Adresse professionnelle :			Ville :		
État/province :		Pays :		Code postal :	
URL :					
Partie 1b. Informations sur la société QSA (le cas échéant)					
Nom de la société :					
Nom du principal contact QSA :			Poste occupé :		
Téléphone :			E-mail :		
Adresse professionnelle :			Ville :		
État/province :		Pays :		Code postal :	
URL :					

Partie 2. Résumé		
Partie 2a. Type d'entreprise du commerçant (cocher toutes les cases adéquates)		
☐ Détaillant	☐ Télécommunications	☐ Épiceries et supermarchés
☐ Pétrole	☐ Commerce électronique	☐ Commande par courrier/téléphone (MOTO)
☐ Autres (préciser) :		
Quels types de réseaux de paiement votre entreprise sert-elle ? ☐ Commande postale/commande par téléphone (MOTO) ☐ Commerce électronique ☐ Carte présente (face à face)	Quels réseaux de paiement sont couverts par cette évaluation ? ☐ Commande postale/commande par téléphone (MOTO) ☐ Commerce électronique ☐ Carte présente (face à face)	

Remarque : *Si votre organisation utilise un réseau ou un processus de paiement qui n'**est** pas couvert par cette évaluation, consultez votre acquéreur ou votre marque de paiement à propos de la validation des autres réseaux.*

Partie 2b. Description de l'entreprise de carte de paiement

Comment et dans quelle mesure votre entreprise stocke-t-elle, traite-t-elle et/ou transmet-elle les données du titulaire de carte ?	

Partie 2c. Emplacements

Énumérer les types de locaux (par exemple, commerces de détail, sièges sociaux, centres de données, centres d'appel, etc.) et un résumé des emplacements inclus dans l'examen PCI DSS.

Type de local	Nombre de locaux de ce type	Emplacement(s) du local (ville, pays)
Exemple : Commerces de détail	*3*	*Boston, Massachusetts, États-Unis*

Partie 2d. Application de paiement

Est-ce que l'organisation utilise une ou plusieurs applications de paiement ? ☐ Oui ☐ Non

Fournir les informations suivantes concernant les applications de paiement utilisées par votre organisation :

Nom de l'application de paiement	Numéro de version	Vendeur de l'application	L'application est-elle listée PA-DSS ?	Date d'expiration du listing PA-DSS (le cas échéant)
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	
			☐ Oui ☐ Non	

Partie 2e. Description de l'environnement

Donner une description ***détaillée*** de l'environnement couvert par cette évaluation. *Par exemple :* • *Connexions entrantes et sortantes à l'environnement de données de titulaires de carte (CDE).*	

• *Composants critiques du système dans le CDE, comme les appareils de POS, les bases de données, les serveurs Web, etc., ainsi que les autres composants de paiement nécessaires, le cas échéant.*	
Est-ce que votre entreprise utilise la segmentation de réseau pour affecter la portée de votre environnement PCI DSS ? *(Consulter la section « Segmentation de réseau » de PCI DSS pour les recommandations concernant la segmentation de réseau)*	☐ Oui ☐ Non

Partie 2f. Prestataires de services tiers

Est-ce que votre société a recours à un intégrateur et revendeur qualifié (QIR) ? Si oui : Nom de la société QIR : Nom individuel QIR : Description des services fournis par QIR :	☐ Oui ☐ Non
Est-ce que votre société partage des données de titulaires de carte avec des prestataires de service tiers (par exemple, intégrateurs et revendeurs qualifiés (QIR), passerelles, services de traitement de paiement, services de prestataires de paiement (PSP), prestataires de services d'hébergement sur le Web, organisateurs de voyages, agents de programmes de fidélisation, etc.) ?	☐ Oui ☐ Non

Si oui :

Nom du prestataire de services :	**Description du service fourni :**

Remarque : *La condition 12.8 s'applique à toutes les entités de cette liste.*

Section 2 : Rapport de conformité

Cette attestation de conformité reflète les résultats d'une évaluation sur site, qui est un document dans un ROC s'y rattachant.

L'évaluation documentée dans cette attestation et dans le ROC a été réalisée le :		
Des contrôles compensatoires ont-ils été utilisés pour répondre à une éventuelle condition du ROC ?	☐ Oui	☐ Non
Avez-vous identifié des conditions du ROC qui n'étaient pas applicables ?	☐ Oui	☐ Non
Des conditions n'ont-elles pas été testées ?	☐ Oui	☐ Non
Des conditions du ROC n'ont-elles pas pu être satisfaites en raison d'une contrainte juridique ?	☐ Oui	☐ Non

Section 3 : Détails d'attestation et de validation

Partie 3. Validation de la norme PCI DSS

Cet AOC dépend des résultats figurant dans ROC en date du *(date d'achèvement du ROC).*

En se basant sur les résultats documentés dans le ROC noté ci-dessus, les signataires identifiés dans les parties 3b-3d, le cas échéant, confirment le statut de conformité suivant pour l'entité identifiée dans la partie 2 de ce document (***cocher la mention applicable) :***

☐	**Conforme :** Toutes les sections du ROC PCI DSS sont remplies, toutes les questions ayant eu une réponse affirmative, ce qui justifie une classification globale comme **CONFORME** ainsi *(nom de la société de commerçant)* a apporté la preuve de sa pleine conformité à la norme PCI DSS.
☐	**Non conforme :** Les sections du questionnaire ROC PCI DSS ne sont pas toutes complétées ou certaines questions n'ont pas une réponse affirmative, ce qui justifie sa classification globale comme **NON CONFORME**, ainsi *(Nom de la société du commerçant)* n'a pas apporté la preuve de sa pleine conformité à la norme PCI DSS. **Date cible** de mise en conformité : Une entité qui soumet ce formulaire avec l'état Non conforme peut être invitée à compléter le plan d'action décrit dans la Partie 4 de ce document. *Vérifier auprès de votre acquéreur ou de la ou des marques de paiement avant de compléter la Partie 4.*
☐	**Conforme, mais avec exception légale :** Une ou plusieurs conditions donnent lieu à une mention « Pas en place » en raison d'une restriction légale qui ne permet pas de respecter la condition. Cette option nécessite un examen supplémentaire de la part de l'acquéreur ou de la marque de paiement. *Si elle est cochée, procéder comme suit :*

Condition affectée	Détails de la manière avec laquelle les contraintes locales empêchent que la condition soit respectée.

Partie 3a. Reconnaissance du statut

Le ou les signataires confirment :

(Cocher toutes les mentions applicables)

☐	Le Rapport sur la conformité a été complété conformément aux *Conditions et procédures d'évaluation de sécurité de la norme PCI DSS*, version *(numéro de version)*, et aux instructions du présent document.
☐	Toutes les informations présentes dans le ROC susmentionné ainsi que dans cette attestation illustrent honnêtement les résultats de mon évaluation à tous points de vue.
☐	J'ai vérifié auprès de mon fournisseur d'application de paiement que mon système de paiement ne stocke pas de données d'authentification sensibles après autorisation.
☐	J'ai lu la norme PCI DSS et je reconnais être tenu de maintenir la pleine conformité à cette norme, ainsi qu'elle s'applique à mon environnement, à tout moment.
☐	Si mon environnement change, je reconnais que je dois procéder à une nouvelle évaluation de mon environnement et implémenter toute condition PCI DSS applicable.

Partie 3a. Reconnaissance du statut (suite)	
☐	Aucune preuve de stockage de données de bande magnétique[1], de données CAV2, CVC2, CID ou CVV2[2], ou de données de code PIN [3]après transaction n'a été trouvée sur AUCUN système examiné pendant cette évaluation.
☐	Les analyses ASV sont effectuées par le fournisseur d'analyse approuvé par le PCI SSC *(nom de l'ASV)*

Partie 3b. Attestation de commerçant	
Signature du représentant du commerçant ↗	*Date :*
Nom du représentant du commerçant :	*Poste occupé :*

Partie 3c. Reconnaissance de l'évaluateur de sécurité qualifié (QSA) (le cas échéant)	
Si un QSA a pris part ou a contribué à cette évaluation, décrire la fonction remplie :	

Signature du cadre supérieur dûment autorisé de la société QSA ↗	*Date :*
Nom du cadre supérieur dûment autorisé :	*Société QSA :*

Partie 3d. Implication de l'évaluateur de sécurité interne (ISA) (le cas échéant)	
Si un ou des ISA ont pris part ou ont contribué à cette évaluation, identifier le personnel ISA et décrire la fonction remplie :	

[1] Données encodées sur la bande magnétique ou données équivalentes sur une puce utilisées pour une autorisation lors d'une transaction carte présente. Les entités ne peuvent pas conserver l'ensemble des données de piste après autorisation des transactions. Les seuls éléments de données de piste pouvant être conservés sont le numéro de compte primaire (PAN), la date d'expiration et le nom du titulaire de carte.

[2] La valeur à trois ou quatre chiffres imprimée sur l'espace dédié à la signature ou au verso d'une carte de paiement, utilisée pour vérifier les transactions carte absente.

[3] Les données PIN (Personal Identification Number, numéro d'identification personnel) saisies par le titulaire de la carte lors d'une transaction carte présente et/ou le bloc PIN crypté présent dans le message de la transaction.

Partie 4. Plan d'action pour les conditions non conformes

Sélectionner la réponse appropriée pour « conforme aux conditions PCI DSS » pour chaque condition. Si votre réponse est « Non » à la moindre condition, vous êtes susceptible de devoir indiquer la date à laquelle votre société s'attend à être conforme à la condition et une brève description des actions prises pour respecter la condition.

Vérifier auprès de votre acquéreur ou de la ou des marques de paiement avant de compléter la Partie 4.

Condition PCI DSS	Description de la condition	Conforme aux conditions de la norme PCI DSS *(Sélectionner un point)*		Date et actions de mise en conformité (si « NON » a été sélectionné pour la moindre des conditions)
		OUI	NON	
1	Installer et gérer une configuration de pare-feu pour protéger les données de titulaires de carte	☐	☐	
2	Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur	☐	☐	
3	Protéger les données de titulaires de carte stockées	☐	☐	
4	Crypter la transmission des données de titulaires de carte sur les réseaux publics ouverts	☐	☐	
5	Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels ou programmes anti-virus	☐	☐	
6	Développer et maintenir des systèmes et des applications sécurisés	☐	☐	
7	Restreindre l'accès aux données de titulaires de carte aux seuls individus qui doivent les connaître	☐	☐	
8	Identifier et authentifier l'accès à tous les composants de système	☐	☐	
9	Restreindre l'accès physique aux données de titulaires de carte	☐	☐	
10	Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaires de carte	☐	☐	
11	Tester régulièrement les processus et les systèmes de sécurité	☐	☐	
12	Gérer une politique de sécurité des informations pour l'ensemble du personnel	☐	☐	

Annexe A2	Conditions supplémentaires de la norme PCI DSS pour les entités utilisant les protocoles SSL/TLS initial pour les connexions POS POI avec carte à des terminaux	☐	☐