BARCLAYS

Obligations de contrôle pour les fournisseurs externes

Norme sur la sécurité des données pour le secteur des cartes de paiement (PCI DSS)

V14.0 – Octobre 2024

Obligation PCI DSS	Description	Raisons de l'importance
1. Conformité des données de la carte	Le fournisseur doit respecter les versions actuelles des normes sur la sécurité des données pour le secteur des cartes de paiement émises par le Payment Security Standards Council (Conseil des normes de sécurité de paiement), par exemple les normes PCI DSS, PA-DSS, PCI-P2PE, PCI-PTS et PCI Card Production.	Protection des données du titulaire de la carte : La norme reconnue en la matière est la norme PCI DSS, une exigence réglementaire mondiale du secteur. Les normes de sécurité PCI sont des exigences techniques et opérationnelles émises par le Payment Card Industry Security Standards Council pour protéger les données du titulaire de la carte.
2. Attestation du fournisseur et du marchand	Le fournisseur doit fournir une attestation de conformité pour les évaluations sur site ou, le cas échéant, un questionnaire d'autoévaluation, portant sur l'étendue des services fournis à Barclays, avant la signature du contrat et chaque année par la suite. Ce processus doit être conforme aux exigences PCI DSS (voir www.pcisecuritystandards.org/) Si des questions sont soulevées concernant l'étendue des services, la description de l'environnement ou la conformité PCI du fournisseur lors de l'examen de l'attestation de conformité, le rapport de conformité sous-jacent peut être demandé et examiné pour obtenir plus d'informations. Un rapport de conformité expurgé peut être accepté s'il confirme que l'étendue de la certification PCI s'applique à l'étendue des services fournis, ou si d'autres questions ont été soulevées par Barclays après examen de l'attestation de conformité. Le fournisseur doit avertir Barclays dès qu'il cesse d'être en conformité, c'est-à-dire dans les plus	Preuve que le fournisseur ou le marchand a obtenu la conformité requise pour les données de carte, pour l'étendue des services fournis à Barclays, et a respecté les exigences adéquates. Preuve que l'attestation de conformité, le rapport de conformité ou le questionnaire d'autoévaluation du fournisseur sont liés au service fourni. Si Barclays fait appel à un fournisseur ou à un marchand qui ne respecte pas les normes PCI DSS, Barclays est tenu de contacter l'équipe Visa Europe Third Party Risk (agentcompliance@visa.com) par e-mail pour confirmer que le fournisseur ou le marchand applique les normes PCI DSS et a soumis à Visa Europe un plan d'état PCI DSS (en utilisant le modèle de Visa Europe) pour examen et approbation.

	brefs délais et au plus 30 jours à compter de la date d'expiration des documents de validation.	
3. Reconnaissance du fournisseur	Le fournisseur doit reconnaître par écrit, auprès de Barclays, avant signature du contrat, qu'il est responsable de la sécurité des données des titulaires de carte pour les services suivants qu'il détient, stocke, traite ou transmet, ou qui sont susceptibles d'avoir une incidence sur la sécurité des données des titulaires de carte clients de Barclays, comme les services de sécurité (serveurs d'authentification, par exemple), hébergement Web, etc. Toute modification du service fourni doit être confirmée par écrit auprès de Barclays avant sa mise en œuvre.	**Extraits de la norme PCI DSS v3.2.1** **Procédure de test pour l'exigence 12.8.2 :** Respecter les accords écrits et confirmer qu'ils incluent une reconnaissance par les fournisseurs de service que ces derniers sont responsables de la sécurité des données des titulaires de carte qu'ils détiennent ou autrement stockent, traitent ou transmettent au nom du client, ou de la mesure dans laquelle ils pourraient avoir une incidence sur la sécurité de l'environnement des données des titulaires de carte du client. Remarque : Conjointement à l'exigence 12.9, cette exigence d'accords écrits entre les organisations et les fournisseurs de service vise à favoriser un niveau cohérent de compréhension entre les parties concernant les responsabilités PCI DSS qui leur incombent. Par exemple, l'accord peut inclure les exigences PCI DSS applicables à respecter dans le cadre du service fourni. **Conseils pour l'exigence 12.8.2 :** La reconnaissance des fournisseurs de service démontre leur engagement à assurer un niveau de sécurité adapté pour les données des titulaires de carte qu'ils ont obtenues de leurs clients. Les procédures et politiques internes des fournisseurs de service liées à leur processus d'engagement des clients et tous les modèles utilisés pour les accords écrits doivent inclure la reconnaissance PCI DSS applicable pour leurs clients. La méthode par laquelle le fournisseur de service fournit la reconnaissance écrite sera décidée conjointement par le fournisseur et ses clients.

Recours à des fournisseurs de service tiers/Externalisation

Un fournisseur de service ou un marchand peut faire appel à un fournisseur de service tiers pour stocker, traiter ou transmettre en son nom les données des titulaires de carte, ou pour gérer les composants tels que les routeurs, les pare-feu, les bases de données, la sécurité physique et/ou les serveurs. Une telle externalisation peut avoir un impact sur la sécurité de l'environnement des données des titulaires de carte.

Les parties doivent clairement identifier les services et composants systèmes inclus dans l'évaluation PCI DSS du fournisseur de service, les exigences PCI DSS spécifiques couvertes par le fournisseur de service et toute exigence qui relève de la responsabilité des clients du fournisseur de service concernant l'inclusion de leurs propres examens PCI DSS. Par exemple, un fournisseur d'hébergement géré doit clairement définir les adresses IP analysées dans le cadre de son processus d'analyse de vulnérabilités trimestriel, ainsi que les adresses IP relevant de la responsabilité de son client et que celui-ci doit inclure dans ses propres analyses trimestrielles.

Les fournisseurs de service doivent démontrer leur conformité aux normes PCI DSS, et les fournisseurs de services de paiement peuvent exiger qu'ils démontrent cette conformité. Les fournisseurs de service doivent contacter leur acquéreur et/ou fournisseur de services de paiement pour déterminer le processus de validation de la conformité approprié.

Les fournisseurs de service tiers peuvent valider la conformité de deux façons :

1) **Évaluation annuelle** : Les fournisseurs de service peuvent faire l'objet d'évaluations PCI DSS annuelles qu'ils conduisent eux-mêmes et fournir à leurs clients la preuve de leur conformité ; ou
2) **Évaluations à la demande** : S'ils ne mènent pas leurs propres évaluations PCI DSS annuelles, les fournisseurs de service doivent faire l'objet d'évaluations à la demande de leurs clients et/ou participer à chaque évaluation PCI DSS de leurs clients. Les résultats de chaque évaluation doivent être transmis aux clients concernés.

Si le tiers fait l'objet de sa propre évaluation PCI DSS, il doit fournir à ses clients une preuve suffisante permettant de vérifier que l'évaluation PCI DSS du fournisseur de service a couvert les services applicables au client, et que les exigences PCI DSS pertinentes ont été étudiées et qu'il a été déterminé qu'elles étaient bel et bien en place. Le type spécifique de preuve fournie par le fournisseur de service à ses clients dépend des accords/contrats en place entre ces parties. Par exemple, la fourniture d'une attestation de conformité et/ou des sections pertinentes du rapport de conformité du fournisseur de service (expurgé pour protéger toute information confidentielle) peut aider à fournir tout ou partie des informations.

De plus, les marchands et fournisseurs de service doivent gérer et surveiller la conformité PCI DSS de tous les fournisseurs de service tiers associés ayant accès aux données des titulaires de carte. *Consulter l'exigence 12.8 dans ce document pour en savoir plus.*