Que faire en cas de compromission

Exigences supplémentaires de Visa

Version 5.0 (Mondial)

À compter d'août 2016

Visa Public

Remarque : Le présent document est un supplément des Règles fondamentales de Visa et des Règles régissant les produits et services de Visa. En cas de conflit entre un contenu du présent document, tout document mentionné dans les présentes, toute annexe du présent document ou toute communication concernant le présent document et tout contenu des Règles fondamentales de Visa et des Règles régissant les produits et services de Visa, les Règles fondamentales de Visa et les Règles régissant les produits et services de Visa s'appliqueront et auront préséance.

Contenu

Contenu

Résumé

La protection du système de paiement est une responsabilité commune. Toutes les parties participant au traitement des données des cartes de paiement ainsi que ceux qui fournissent des services susceptibles d'influencer les données des cartes de paiement doivent au moins préserver la conformité aux exigences de la norme relative à la sécurité des données de l'industrie des cartes de paiement (PCI DSS). Les entités qui soupçonnent ou qui ont confirmé des données de compte compromises, sont tenues de prendre des mesures rapides pour prévenir une autre exposition des données des cartes de paiement et de veiller à la mise en place et au bon fonctionnement de contrôles appropriés concernant le respect de la norme PCI DSS et la sécurité du NIP de la norme PCI. Les données de compte compromises ne sont pas limitées aux instructions du réseau et les procédures et échéances s'appliquent également aux compromissions mettant en cause la falsification ou le copiage des appareils de saisie du NIP (ASN) au niveau du point de vente (PDV).

Le présent document contient des procédures obligatoires et des échéances à respecter concernant l'établissement de rapports et l'intervention en cas de compromission, suspecte ou avérée, des données de compte.

Mesures à prendre pour les entités potentiellement compromises

Conserver les éléments de preuve

Pour identifier les causes profondes et faciliter les enquêtes, il est important de s'assurer de l'intégrité des composants du système et de l'environnement en conservant tous les éléments de preuve.

- Évitez d'accéder aux systèmes compromis ou de modifier ceux-ci (par exemple, ne vous connectez pas aux systèmes compromis et ne changez pas les mots de passe; ne vous connectez pas avec des identifiants administratifs). Visa recommande fortement de mettre hors ligne les systèmes compromis immédiatement et de ne pas les utiliser pour le traitement des paiements ou interagir avec les systèmes de traitement des paiements.
- Évitez d'éteindre ou de redémarrer les systèmes compromis. Isolez plutôt les systèmes compromis du reste du réseau en débranchant les câbles de réseau ou par d'autres moyens.
- Identifiez tous les composants compromis suspects et consignez-les (par exemple, les ordinateurs de bureau, les serveurs, les terminaux, les journaux, les événements de sécurité, les bases de données, les segments de recouvrement des ASN, etc.).
- Consignez les mesures de confinement et de correction, notamment les dates et les heures (de préférence en TUC), les personnes en cause et les détails des mesures prises.
- Conservez toutes les preuves et tous les journaux (par exemple, les preuves originales telles que la copie-image des systèmes et des logiciels malveillants, les événements de sécurité, les blogues, les protocoles de bases de données, les journaux du pare-feu, etc.).

Fournir le rapport d'enquête initiale de Visa

Dans les trois (3) jours ouvrables suivant la compromission, suspecte ou avérée, des données de compte, fournissez le rapport d'enquête initiale de Visa – commençant à la page 4 – à la banque acquéreuse ou directement à Visa.

Exécuter le plan de notification

Avisez immédiatement toutes les parties concernées, y compris :

- votre équipe d'intervention en cas d'incident interne et votre groupe de sécurité de l'information.
- votre banque de marchand (appelée également acquéreur ou banque acquéreuse).
  - Si vous ne connaissez pas le nom ou les coordonnées de votre banque de marchand, demandez assistance à l'équipe de gestion des risques de Visa :

    États-Unis – +1 650 432-2978 ou USFraudControl@visa.com

    Canada – +1 416 860-3872 ou CanadaInvestigations@visa.com

    Amérique latine et Caraïbes – +1 305 328-1593 ou LACFraudInvestigations@visa.com

    Asie-Pacifique, Europe centrale et orientale, Moyen-Orient et Afrique – VIFraudControl@visa.com

- Le fabricant de l'appareil de paiement affecté si vous estimez que l'incident implique la compromission d'un appareil de saisie du NIP (ASN), particulièrement s'il s'agit d'un appareil approuvé selon les exigences de la norme PCI relatives à la sécurité des transactions de paiement (STP).
- Le service juridique pour déterminer si les lois rendant obligatoire la notification du client sont applicables. Il vous est fortement recommandé également d'aviser immédiatement :
- L'organisme d'application de la loi concerné en cas de compromission des données de compte.
- L'organisme fédéral d'application de la loi si la compromission a lieu aux États-Unis. L'organe Electronic Crimes Task Forces (ECTF) du Secret Service américain a pour mission principale de mener des enquêtes sur les crimes financiers; de plus, il peut apporter son aide en intervenant en cas d'incident et en atténuant la compromission des données de compte.

  Visitez www.secretservice.gov/investigation pour obtenir les coordonnées du bureau su le terrain d'ECTF.

Mener une enquête judiciaire

Visa peut demander à une entité compromise de faire appel à un enquêteur judiciaire PCI pour mener une enquête judiciaire indépendante. Si l'enquête judiciaire est recommandée, il faut suivre la démarche ci-après.

Dès la constatation de la compromission de données de compte, ou à la réception d'un avis d'enquête judiciaire indépendante, une entité doit :

- Recourir à un enquêteur judiciaire PCI (ou signer un contrat) dans les cinq (5) jours suivants.
- Fournir à Visa le rapport judiciaire initial (préliminaire) dans les dix (10) jours ouvrables suivant le recours aux services de l'enquêteur judiciaire PCI (ou la signature du contrat).
- Fournir à Visa le rapport judiciaire final dans les dix (10) jours ouvrables suivant l'accomplissement de l'examen.

L'enquêteur judiciaire PCI ne doit pas être une organisation affiliée à l'entité compromise ou avoir fourni des services à celle-ci dans le cadre d'une enquête judiciaire PCI précédente ou à titre d'évaluateur autorisé en sécurité (ÉAS), de conseiller, de consultant ou encore s'il a fourni un soutien en matière de surveillance ou de sécurité de réseau, etc.

Visa n'acceptera pas des rapports judiciaires provenant d'organisations judiciaires PCI non approuvées. Les enquêteurs judiciaires PCI sont tenus de fournir les rapports judiciaires et les conclusions de l'enquête directement à Visa.

Une liste des organisations PCI approuvées est accessible sur le site :
www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

Fournir tous les comptes exposés

Tous les comptes Visa compromis (connus ou suspectés) doivent être téléversés dans le système de gestion des comptes compromis (SGCC) dans un délai de cinq (5) jours ouvrables suivant la première des éventualités suivantes : (a) la date à laquelle Visa demande des numéros de compte, (b) la constatation d'une fenêtre d'exposition, ou (c) la découverte de données de compte compromises.

- Les entités doivent collaborer avec leur banque acquéreuse pour téléverser les comptes.
- Pour en savoir davantage ou demander de l'aide, écrivez à Visa à l'adresse : CAMS@Visa.com

Rapport d'enquête initiale de Visa

Dès qu'elles sont avisées de la compromission, suspecte ou avérée, des données de compte, les entités compromises doivent déclencher une enquête préliminaire de tous les systèmes potentiellement affectés et de ceux des fournisseurs de services tiers. Les entités compromises doivent partager les conclusions de l'enquête avec Visa ainsi qu'avec la banque acquéreuse, le cas échéant. Une enquête préliminaire n'est pas la même que le rapport préliminaire de l'enquêteur judiciaire PCI. L'enquête initiale permettra à Visa de comprendre l'environnement en réseau de l'entité compromise et de l'ampleur potentielle de l'incident.

Pour se conformer aux exigences d'enquête de Visa, l'entité doit soumettre, de manière sécuritaire, (par exemple, chiffrement, codage PGP, courriel sécurisé sur Visa Online, etc.) les renseignements ci-après, et ce, dans les trois (3) jours ouvrables suivant la compromission, suspecte ou avérée, des données de compte.

Rapport d'enquête de Visa	
Nom de l'entité :	
Type de l'entité :	
NIB(s) du ou des acquéreur(s) : (Citer tous les cas qui s'appliquent)	
L'entité envoie-t-elle des transactions à une entité de traitement?	☐ **Oui** ☐ **Non** *(Si oui, joignez la liste des entités de traitement contenant leurs noms et leurs coordonnées. Si l'entité qui fait le rapport est également chargée du traitement, veuillez fournir la liste de tous les NIB acquéreurs et les noms de tous les marchands, les ID des accepteurs de carte de marchand, la ville et l'État).*
Niveau PCI DSS de l'entité *(p. ex., niveau 1 à 4) :*	
Statut de conformité de l'entité à la norme PCI DSS :	*(si l'entité est en conformité avec la norme PCI DSS, veuillez joindre les documents justificatifs pertinents.)*
Le nombre approximatif des transactions traitées par an	• GAB • NIP/débit PDV • Crédit
L'entité du marchand est-elle détenue par une société ou s'agit-il d'une franchise individuelle?	*(Si le marchand a d'autres emplacements, veuillez joindre une liste.)*
Nom des applications et des versions de paiement :	• • • •

<table>
<tr><td rowspan="4">Identifier la ou les parties responsables de la configuration et de la prise en charge de la solution du point de vente (PDV)
(p. ex., intégrateur, revendeur ou agent).</td><td>NOM</td><td>TITRE</td><td>COORDONNÉES</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="4">(Si l'entité est un intégrateur ou un revendeur, veuillez joindre la liste de tous les NIB des acquéreurs ainsi que les noms des marchands, les ID des accepteurs de carte du marchand, la vile et l'État.)</td></tr>
<tr><td>S'agit-il d'une application ou d'une version de paiement mandatée par une société ou une franchise?</td><td colspan="3"></td></tr>
<tr><td>Le terminal fonctionne-t-il sur un ordinateur de bureau ou est-il connecté à un environnement de bureau personnel?</td><td colspan="3"></td></tr>
<tr><td>Peut-on se connecter à distance à l'environnement de l'entité?</td><td colspan="3">☐ Oui ☐ Non
Si oui, quelles sont les organisations qui ont l'accès à distance?
•
•</td></tr>
<tr><td>Quel type de solution d'accès à distance utilise-t-on?</td><td colspan="3"></td></tr>
<tr><td>L'accès à distance est-il toujours activé ou est-il accessible sur demande?</td><td colspan="3"></td></tr>
<tr><td>L'appareil du point de vente fonctionne-t-il avec EMV?</td><td colspan="3">☐ Oui ☐ Non
Si oui, veuillez indiquer le nom et le numéro du modèle.</td></tr>
<tr><td>La solution PDV fonctionne-t-elle avec le chiffrement point à point?</td><td colspan="3">☐ Oui ☐ Non
Si oui, précisez.</td></tr>
<tr><td>L'entité accepte-t-elle le NIP?</td><td colspan="3">☐ Oui ☐ Non</td></tr>
<tr><td>L'appareil de saisie du NIP (ASN) de l'entité est-il approuvé selon les exigences de la norme PCI relatives à la sécurité des transactions de paiement (STP); et figure-t-il sur le site Web de PCI SSC?</td><td colspan="3">☐ Oui ☐ Non
Indiquez le modèle de l'ASN, le matériel informatique, le micrologiciel et les numéros d'application et de version. Visitez www.pcisecuritystandards.org/pin pour obtenir la liste des appareils de saisie du NIP approuvés selon les exigences de la norme PCI relatives à la sécurité des transactions de paiement (STP).</td></tr>
</table>

L'entité est-elle colocalisée ou hébergée?	Si elle est hébergée, indiquez le nom et les coordonnées du fournisseur d'hébergement.
Donnez des renseignements sur l'application et la version du panier d'achat, le cas échéant.	
Décrivez tout changement récent ayant touché le réseau ou les systèmes.	• Mises à niveau de l'application des paiements ☐ Oui ☐ Non • Installation d'un pare-feu ☐ Oui ☐ Non • Installation d'un programme antivirus ☐ Oui ☐ Non • Changements apportés à l'authentification de l'accès à distance ☐ Oui ☐ Non AUTRE : • • •
L'entité a-t-elle reçu des plaintes de ses clients concernant les transactions frauduleuses?	☐ **Oui** ☐ **Non** Si oui, veuillez préciser.
Un organisme d'application de la loi a-t-il pris contact avec l'entité à propos de transactions frauduleuses?	☐ **Oui** ☐ **Non** Si oui, indiquez les dates et l'organisme d'application de la loi. • • •
Si la compromission des données de compte est avérée, veuillez fournir les renseignements ci-après	
Comment et quand a-t-on identifié l'incident?	
Dans quelles circonstances la compromission a-t-elle eu lieu?	Joignez les documents ci-après, le cas échéant : • Liste des vulnérabilités ayant causé la compromission ou qui y ont contribué. • Exemple de tout courriel d'hameçonnage • Détails de l'activité non autorisée • Liste des IP malveillants • Information sur le logiciel malveillant, le cas échéant.

L'entité a-t-elle avisé l'organisme d'application de la loi?	☐ **Oui** ☐ **Non** Si oui, de quel organisme s'agit-il et quand était-il avisé? Indiquez les coordonnées le cas échéant.
Si vous connaissez l'organisme, précisez le nombre de cartes Visa compromises (comptes devenus vulnérables à la suite de la violation de la sécurité des données).	
Les comptes affectés ont-ils été téléversés dans le système de gestion des comptes compromis (SGCC)?	
Quelles sont les données compromises ou exposées?	☐ **Numéro de compte primaire** ☐ **Date d'expiration (NCP)** ☐ **Piste complète 1 ou 2** ☐ **NIP** ☐ **CVV2** Renseignements d'identification personnelle du titulaire de carte (RIP) ☐ **Nom du titulaire de carte** ☐ **Numéro d'assurance sociale** ☐ **Date de naissance** ☐ **Autre :**
A-t-on résolu le cas de compromission? Si oui, comment?	☐ **Oui** ☐ **Non** Si oui, comment?

Étapes et exigences pour les membres de Visa

Conformément aux dispositions des Règles fondamentales et des Règles sur les produits et services de Visa (Règles de Visa) et en vertu du présent document Que faire en cas de compromission, les membres de Visa sont tenus de mener une enquête approfondie sur les cas, avérés ou suspects, de perte, de vol ou de compromission du compte Visa ou des renseignements sur les titulaires de carte mettant en cause soit leur propre environnement en réseau, soit celui de leur(s) marchand(s) ou agent(s).

Les Règles de Visa contiennent des mécanismes d'application de la loi auxquels Visa peut recourir en cas de violation des Règles de Visa. Les Règles de Visa précisent les procédures à suivre pour mener une enquête en cas de violation ainsi que les règles et les calendriers concernant les évaluations de la non-conformité.

Les Règles de Visa sont accessibles sur le site Visa.com.

Avis

1. Tout accès non autorisé, suspect ou avéré, aux données du titulaire de carte de Visa doit être signalé immédiatement au groupe de gestion des risques de Visa.
2. Il y a lieu de fournir à Visa, dans un délai de 48 heures, le statut de conformité à la norme PCI DSS et, le cas échéant, le statut de conformité à l'égard des exigences de la norme de sécurité des données de l'application des paiements (PA-DSS) et des exigences de la norme PCI relative à la sécurité du NIP, et ce, au moment de l'incident.

Enquête initiale (dans les trois jours ouvrables suivants)

3. Les membres sont tenus de procéder à une enquête initiale et de fournir le rapport d'enquête initiale de Visa (contenant les constatations et les conclusions) à Visa dans un délai de trois (3) jours ouvrables. L'information permettra à Visa de comprendre le risque potentiel et de contenir l'incident. La documentation doit comporter toutes les étapes suivies pour contenir l'incident.

Enquête judiciaire indépendante

4. Visa peut, à sa discrétion, demander à l'entité compromise de mener une enquête judiciaire indépendante en cas d'exposition suspecte des données du titulaire de carte. L'enquête doit être menée par un enquêteur judiciaire PCI. Visa peut demander à l'entité compromise de mener une enquête PCI en raison des facteurs suivants notamment :

- Perte pour cause de fraude liée aux rapports concernant les points d'achat communs.
- Violation de la sécurité des données affectant les cartes de paiement déclarée par l'intéressé.
- Nombre de sources signalant l'entité comme étant potentiellement compromise.
- Les rapports de l'organisme d'application de la loi ou d'une autre source crédible concernant une violation de la sécurité des données affectant les cartes de paiement.

- Une entité qui n'a pas contenu l'incident initial ou précédent (on peut détecter ce genre de cas en examinant les rapports relatifs aux points d'achat communs, en analysant les données ou par d'autres moyens).
- Fournisseur de services, agent, intégrateur, revendeur, etc. ayant un accès à distance aux multiples emplacements.

5. Un membre de visa ou une entité compromise doit recourir aux services d'un enquêteur judiciaire PCI pour mener une enquête judiciaire.
   Visa n'acceptera PAS les rapports judiciaires provenant de sociétés judiciaires PCI non approuvées. Il incombe au membre de Visa de s'assurer que son marchand ou son agent a recours à un enquêteur judiciaire PCI pour mener une enquête.
6. Visa a le droit de faire appel directement aux services d'un enquêteur judiciaire PCI pour mener une enquête si elle le juge nécessaire. Dans ce cas, Visa imputera tous les coûts de l'enquête au membre concerné. Les coûts de l'enquête peuvent s'ajouter à toute évaluation applicable de la non-conformité effectuée par Visa.
7. Dès la constatation de la compromission de données de compte, ou à la réception d'un avis d'enquête judiciaire indépendante provenant de Visa, un membre doit :

- s'assurer de recourir à un enquêteur judiciaire PCI (ou s'assurer que le contrat est signé) dans un délai de cinq (5) jours ouvrables.
- s'assurer que le travail initial est en cours et fournir à Visa le rapport judiciaire initial (préliminaire) dans les dix (10) jours ouvrables suivant le recours aux services de l'enquêteur judiciaire (ou la signature du contrat).
- fournir à Visa le rapport judiciaire final dans les dix (10) jours ouvrables suivant l'accomplissement de l'examen.

8. L'enquêteur judiciaire PCI est tenu de communiquer les rapports d'enquête judiciaire ainsi que les conclusions à Visa.
9. **Remarque :** Visa a le droit de rejeter le rapport d'un enquêteur judiciaire PCI s'il ne répond pas aux exigences établies dans le guide du programme de l'enquêteur judiciaire PCI. Les enquêteurs judiciaires PCI sont tenus de résoudre avec Visa, l'acquéreur et l'entité compromise, toute anomalie avant la finalisation du rapport.
10. Pour de plus amples renseignements sur les lignes directrices relatives à l'enquête judiciaire, veuillez consulter le Guide du programme de l'enquêteur judiciaire PCI, qui est accessible sur le site www.pcisecuritystandards.org/document_library (Filtrer par : PFI)
11. Liste des enquêteurs judiciaires PCI approuvés : https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators
12. En cas de compromission suspecte du NIP, l'enquêteur judiciaire PCI doit effectuer une enquête sur la sécurité du NIP et la gestion de clé ainsi qu'une évaluation de la sécurité du NIP de la norme PCI.
13. **Remarque :** Si le recours aux services d'un enquêteur judiciaire PCI ne se fait pas fait selon les exigences susmentionnées, il sera considéré comme étant une violation des Règles de Visa et le présent document ainsi que les évaluations de non-conformité peuvent être appliqués.

Données des comptes exposés

14. Fournir tous les comptes exposés – tous les comptes Visa compromis (connus ou suspectés) doivent être téléversés dans le système de gestion des comptes compromis (SGCC) dans un délai de cinq (5) jours ouvrables suivant la première des éventualités suivantes : (a) la date à laquelle Visa demande des numéros de compte, (b) la constatation d'une fenêtre d'exposition, ou (c) la découverte de données de compte compromises.

    Pour demander de l'aide ou l'accès, écrivez à : CAMS@Visa.com

    Toutes les parties qui téléversent des comptes à risque doivent inclure les renseignements suivants :

- Nom de l'entité
- Fenêtre d'exposition
- Données à risque (par exemple, numéro de compte primaire (PAN), Piste 1 ou Piste 2, CVV2, NIP, date d'expiration, etc.
- Numéro d'identification bancaire (NIB) (le cas échéant)
- Code de catégorie du marchand (CCM) (le cas échéant)
- Nom de l'enquêteur de l'organisme d'application de la loi et le numéro d'incident (le cas échéant)
- Nom de l'enquêteur (le cas échéant)
- Numéro d'incident (le cas échéant)

Conforme à la norme PCI DSS

15. Les entités compromises doivent se conformer pleinement à la norme PCI notamment en respectant les exigences de la norme relative à la sécurité des données de l'industrie des cartes de paiement (PCI DSS), la norme de sécurité des données de l'application des paiements (PA-DSS) et, le cas échéant, les exigences en matière de sécurité du NIP de la norme PCI .

    Remarque : Si à la suite d'un audit de la conformité de la norme PCI DSS effectué par un évaluateur agréé en sécurité (ÉAS) commandité par une entité compromise, il s'est avéré que les données de compte de celle-ci ont été compromises, Visa demandera à l'entité concernée de recourir à un autre ÉAS pour effectuer un audit en la matière, et ce, après que toutes les mesures de correction aient été prises.

    Veuillez visiter www.pcisecuritystandards.org pour en apprendre davantage sur la norme PCI DSS et le programme de vérification des appareils de saisie du NIP.

    Pour obtenir de plus amples renseignements sur les exigences de la norme PCI relatives à la sécurité du NIP, veuillez visitez le site www.visa.com/pinsecurity.

Annexe : Consultation rapide par sujet

Entité compromise

Éléments de preuve	Voir la section Conserver les éléments de preuve, page 2
Enquêtes	Voir les sections Fournir le rapport d'enquête initiale de Visa (page 2) et Mener une enquête judiciaire (page 3)
Téléverser les comptes exposés	Voir la section Fournir des comptes exposés, page 3
PCI DSS	Voir la section Conformité à la norme PCI DSS, page 10

Membre Visa

Règles de Visa	Voir la section Étapes et exigences, page 8
Avis	Voir Avis, page 8
Enquêtes	Voir Enquête initiale et enquête judiciaire indépendante, page 8
Fournir les comptes exposés	Voir la section Données de comptes exposés, page 9
PCI DSS	Voir la section Conformité à la norme PCI DSS, page 10