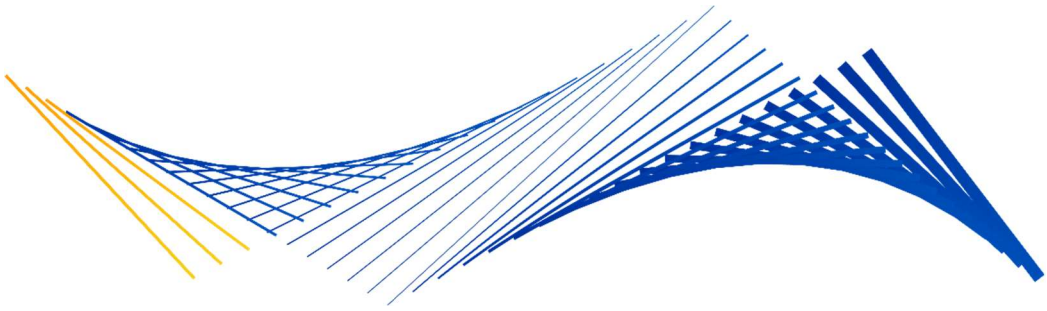
Quoi faire en cas de compromission

Exigences supplémentaires de Visa

Version 6.0

En vigueur depuis le 19 octobre 2019



Remarque importante sur les droits d'auteurs

À propos des exigences supplémentaires de Visa

Le présent document est un supplément aux *Règles fondamentales Visa et au Règlement sur les produits et services de Visa*. En cas de conflit entre le contenu du présent document, un document mentionné dans le présent document, une pièce jointe au présent document ou toute communication concernant le présent document et le contenu des *Règles fondamentales Visa et du Règlement sur les produits et services de Visa*, ces derniers gouvernent et ont préséance.

Pour les exigences européennes de Visa, contactez datacompromise@visa.com

Contenu

Résumé

Visa s'engage à promouvoir la sécurité et la prospérité à long terme du système de paiement Visa. À cette fin, Visa vise à assurer la résolution en temps opportun des événements de compromission de données externes, à notifier les comptes à risque afin d'endiguer les impacts de la fraude, et à synthétiser les preuves judiciaires, les renseignements et l'analyse de la fraude afin de formuler des plans de correction qui renforcent l'efficacité du système de paiement.

La protection de l'écosystème des paiements est une responsabilité partagée. Toute entité qui stocke, traite ou transmet des données de cartes de paiement ou qui a accès à ces systèmes ou à ces données, est tenue d'adhérer et de maintenir la conformité à toutes les exigences de la norme relative à la sécurité des données de l'industrie des cartes de paiement (PCI DSS).

Le document présent de Visa intitulé *Quoi faire en cas de compromission* est un guide basé sur les exigences qui s'applique aux entités qui soupçonnent ou qui ont subi un événement compromettant pour leurs systèmes de paiement, ou pour des systèmes de paiement dont elles assurent le service ou le soutien. Cela comprend, sans s'y limiter, toutes les institutions financières membres de Visa (c.-à-d. les émetteurs et les acquéreurs), les marchands, les opérateurs de traitement, les passerelles, les agents, les fournisseurs de services, les vendeurs tiers, les revendeurs, les intégrateurs et toutes les autres entités, ainsi que les autres participants au système de paiement, qui exploitent un environnement de paiement ou y accèdent.

Le présent document établit des procédures et des délais pour signaler et répondre à un événement de compromission suspecté ou confirmé. Pour atténuer le risque lié au système de paiement lors d'un événement compromettant, il est nécessaire d'agir rapidement afin d'éviter toute exposition supplémentaire, notamment en assurant des actions de limitation et de remédiation, comme s'assurer que les contrôles PCI DSS et de sécurité du NIP PCI appropriés sont en place et fonctionnent correctement.

Exigences pour les entités qui soupçonnent ou ont confirmé un événement de compromission

Toute entité qui soupçonne ou confirme un accès non autorisé aux données du titulaire de la carte Visa, notamment toute entité qui stocke, traite ou transmet des données sur les titulaires de la carte ou qui a accès à un environnement ou à des systèmes de paiement, est tenue de se conformer aux exigences du présent document.

Cela comprend, sans s'y limiter, toutes les institutions financières membres de Visa (c.-à-d. les émetteurs et les acquéreurs), les marchands, les opérateurs de traitement, les passerelles, les agents, les fournisseurs de services, les vendeurs tiers, les revendeurs, les intégrateurs et toutes les autres entités, ainsi que les autres participants au système de paiement, qui exploitent un environnement de paiement ou y accèdent.

1. Envoyer une notification à Visa dans un délai de trois (3) jours civils

1.1. Une entité qui soupçonne ou confirme un accès non autorisé aux données d'un compte de paiement Visa ou à tout système de paiement qui stocke, traite ou transmet des données de compte de paiement Visa, doit s'assurer que le cas de compromission est signalé au groupe de gestion des risques de Visa dans les trois (3) jours civils qui suivent (a) la découverte d'éléments de preuve suffisants pour soulever un doute raisonnable quant à l'existence d'un cas de compromission ; (b) la découverte de preuves suffisantes pour confirmer l'existence d'un cas de compromission au-delà d'un doute raisonnable. Les institutions financières membres de Visa sont chargées de veiller à la conformité de cette exigence par leurs sociétés affiliées, leurs agents et leurs clients.

Cette notification doit être adressée au bureau régional de l'équipe de gestion des risques de Visa :

Amérique du Nord (AN)	USFraudControl@visa.com
Amérique latine et Caraïbes (ALC)	LACFraudInvestigations@visa.com
Asie-Pacifique (AP) Europe centrale et orientale, Moyen-Orient et Afrique (ECMOA)	USFraudControl@visa.com
Assistance d'urgence 24/7 du Centre des opérations de gestion des risques	Numéro sans frais : 1 844-847-2106 International : 1 650-432-3379

Remarque : *Les acquéreurs Visa ayant accès à l'outil de gestion des enquêtes mondiales (GIMT) de Visa doivent fournir un avis par l'entremise de GIMT*

L'outil de gestion des enquêtes mondiales (GIMT) de Visa est une solution de gestion de cas de bout en bout qui sert de dépôt central pour la réception et la distribution de l'information d'enquête sur les événements de compromission et autres stratagèmes frauduleux. Les

acquéreurs et leurs chargés du traitement de tiers (TPP) désignés sont tenus d'utiliser GIMT pour gérer les cas Visa. Pour plus de détails, veuillez vous référer au *Guide de l'acquéreur GIMT de Visa* sur Visa en ligne.

2. Effectuer une enquête initiale et fournir un rapport d'incident

2.1. Dans les trois (3) jours civils suivant la notification à Visa conformément à la section 1.1. ci-dessus, fournir un rapport décrivant l'événement (le rapport d'incident) à Visa et à la banque acquéreuse (le cas échéant). Veuillez consulter l'annexe A à la fin du document pour obtenir une copie modifiable du rapport d'incident.

2.2. Les informations fournies dans le rapport d'incident aident Visa à comprendre l'environnement réseau de l'entité compromise, la portée et l'exposition potentielles de l'incident, et à contenir l'événement. La documentation doit inclure toutes les mesures prises pour contenir et remédier à l'événement.

Ce rapport d'incident doit être adressé au bureau régional de l'équipe de gestion des risques de Visa :

Amérique du Nord (AN)	USFraudControl@visa.com
Amérique latine et Caraïbes (ALC)	LACFraudInvestigations@visa.com
Asie-Pacifique (AP) Europe centrale et orientale, Moyen-Orient et Afrique (ECMOA)	USFraudControl@visa.com
Assistance d'urgence 24/7 du Centre des opérations de gestion des risques	Numéro sans frais : 1 844-847-2106 International : 1 650-432-3379

Remarque : *Les acquéreurs Visa ayant accès à l'outil de gestion des enquêtes mondiales (GIMT) de Visa doivent fournir un avis par l'entremise du GIMT*

3. Fournir un avis aux autres parties concernées

3.1. Notifier immédiatement toutes les parties concernées, y compris, mais sans s'y limiter, la banque acquéreuse (le cas échéant).

3.2. Si le nom ou les coordonnées de votre banque acquéreuse sont inconnus, veuillez communiquer avec l'un des bureaux régionaux de l'équipe de gestion des risques de Visa :

Amérique du Nord (AN)	USFraudControl@visa.com
Amérique latine et Caraïbes (ALC)	LACFraudInvestigations@visa.com
Asie-Pacifique (AP) Europe centrale et orientale, Moyen-Orient et Afrique (ECMOA)	USFraudControl@visa.com
Assistance d'urgence 24/7 du Centre des opérations de gestion des risques	Numéro sans frais : 1 844-847-2106 International : 1 650-432-3379

3.3. Il est fortement recommandé d'en informer immédiatement :

3.3.1. Votre équipe interne de réponse aux incidents et votre groupe de sécurité de l'information.

3.3.2. Le fabricant de votre PED (appareil de saisie NIP), s'il est déterminé que l'incident implique la compromission d'un PED, en particulier s'il s'agit d'un appareil approuvé par

PCI PTS.

3.3.3. Votre service juridique, en particulier si la loi applicable impose la notification du client.

3.3.4. Les organismes d'application de la loi locaux ou nationaux appropriés.

3.3.5. L'Electronic Crimes Task Forces (ECTF) des services secrets des États-Unis, si l'événement compromettant se situe aux États-Unis. L'ECTF se concentre sur les enquêtes relatives aux crimes financiers et peut fournir une assistance face à un cas de compromission. Visitez-le www.secretservice.gov/investigation/ for ECTF field office contact information.

4. Fournir à Visa les données exposées sur les comptes de paiement

4.1. Dans les trois (3) jours civils suivant l'un des scénarios suivants : (a) la découverte de données de compte compromises ; (b) la date à laquelle Visa demande les numéros de compte ; ou (c) la détection d'une fenêtre d'exposition, les entités sont tenues de s'assurer que tous les numéros de compte Visa compromis (connus ou soupçonnés) sont fournis à l'équipe de gestion des risques de Visa par l'entremise de l'outil de gestion des enquêtes mondiales (GIMT) ou du système de gestion des comptes compromis (CAMS) de Visa.

4.1.1. Les entités doivent collaborer avec leur acquéreur officiel pour télécharger les comptes vers GIMT ou CAMS, le cas échéant.

4.1.2. Pour obtenir de plus amples renseignements ou de l'aide, veuillez communiquer avec le bureau régional de l'équipe de gestion des risques de Visa :

Amérique du Nord (AN)	USFraudControl@visa.com
Amérique latine et Caraïbes (ALC)	LACFraudInvestigations@visa.com
Asie-Pacifique (AP) Europe centrale et orientale, Moyen-Orient et Afrique (ECMOA)	USFraudControl@visa.com
Assistance d'urgence 24/7 du Centre des opérations de gestion des risques	Numéro sans frais : 1 844-847-2106 International : 1 650-432-3379

5. Mener une enquête judiciaire PCI

5.1. Visa peut demander, à sa discrétion, à une entité compromise de faire appel à un enquêteur judiciaire PCI pour mener une enquête judiciaire indépendante. L'enquête doit être effectuée par un enquêteur judiciaire et les éléments suivants sont requis :

5.1.1. Fournir un soutien logistique et technique complet à l'enquêteur pour faciliter l'achèvement rapide de l'enquête, y compris, mais sans s'y limiter, des mises à jour régulières de l'état d'avancement, la participation à des conférences téléphoniques avec toutes les parties, la fourniture d'échantillons de logiciels malveillants et d'indicateurs de compromission, etc.

5.1.2. Dans les cinq (5) jours ouvrables, signer un contrat pour retenir les services d'un enquêteur judiciaire pour effectuer une enquête PCI et informer Visa du nom de la société judiciaire et de l'enquêteur principal. Le cas échéant, l'entité doit également informer la banque acquéreuse qu'elle a retenu les services d'un enquêteur judiciaire et lui fournir le nom de la société et de l'enquêteur principal.

5.1.3. Dans les cinq (5) jours ouvrables suivants le moment où l'entité a retenu les services d'un

enquêteur judiciaire et signé un contrat, fournir à Visa le rapport judiciaire initial (c.-à-d. préliminaire).

5.1.4. Dans les dix (10) jours ouvrables suivant la fin de l'enquête judiciaire, fournir à Visa un rapport judiciaire final.

5.2. Les circonstances impliquant des entités à haut risque, qui comprennent, sans s'y limiter, les marchands de niveau 1 et 2, les opérateurs de traitement, les passerelles, les agents, les fournisseurs de services, les vendeurs tiers, les intégrateurs, les revendeurs ainsi que d'autres participants au système de paiement opérant ou accédant à distance à un environnement de paiement, présentent un risque inhérent plus élevé pour l'écosystème de paiement et peuvent nécessiter le recours à un enquêteur judiciaire PCI.

5.3. L'enquêteur ne peut provenir d'une société judiciaire qui est affiliée à l'entité compromise ou qui a fourni des services à l'entité compromise, comme une enquête précédente de l'enquêteur, un évaluateur de sécurité qualifié (QSA), un conseiller, un consultant, une surveillance ou un support de sécurité réseau, au cours des 3 dernières années.

5.4. Visa n'acceptera pas les rapports judiciaires provenant de sociétés non approuvées. Les enquêteurs sont tenus de fournir les rapports d'expertise judiciaire et les résultats d'enquête directement à Visa.

5.5. Visa se réserve le droit de rejeter les rapports d'enquête qui ne satisfont pas aux exigences du présent document et d'exiger une nouvelle enquête judiciaire. Une nouvelle enquête judiciaire sera aux frais de l'entité et non de Visa.

Une liste des enquêteurs judiciaires approuvés est disponible à l'adresse suivante

www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

6. Mener une enquête indépendante

6.1. Ce ne sont pas tous les cas de compromission qui nécessitent une enquête judiciaire. Visa peut exiger qu'une entité potentiellement compromise mène une enquête indépendante au lieu de, ou avant, une enquête judiciaire PCI. Si elle est informée qu'une enquête indépendante est nécessaire, une entité est tenue de faire ce qui suit :

6.1.1. Dans les cinq (5) jours ouvrables, signer un contrat pour retenir les services d'un enquêteur pour effectuer une enquête indépendante et fournir à Visa le nom de l'entreprise et de l'enquêteur principal. Le cas échéant, l'entité doit informer la banque acquéreuse.

6.1.2. Dans les cinq (5) jours ouvrables suivant l'exécution du contrat, fournir à Visa le rapport initial (c'est-à-dire préliminaire).

6.1.3. Dans les dix (10) jours ouvrables suivant la fin de l'enquête, fournir à Visa un rapport final.

6.1.4. Fournir un soutien logistique et technique complet à l'enquêteur pour faciliter l'achèvement rapide de l'enquête, y compris, mais sans s'y limiter, des mises à jour régulières de l'état d'avancement, la participation à des conférences téléphoniques avec toutes les parties, la fourniture d'échantillons de logiciels malveillants et d'indicateurs de compromission, etc.

6.2. L'enquêteur ne peut provenir d'une société qui est affiliée à l'entité compromise ou qui a

fourni des services à l'entité compromise, comme une enquête précédente de l'enquêteur, un évaluateur de sécurité qualifié (QSA), un conseiller, un consultant, une surveillance ou un support de sécurité réseau, au cours des 3 dernières années.

6.3. Les enquêteurs indépendants sont tenus de fournir les rapports d'enquête indépendante et les autres résultats d'enquête directement à Visa.

6.4. Visa se réserve le droit de rejeter les rapports d'enquête qui ne satisfont pas aux exigences du présent document et d'exiger une nouvelle enquête judiciaire.

7. Conserver les éléments de preuve

7.1. Pour identifier la cause première d'un cas de compromission potentiel, faciliter les enquêtes et garantir l'intégrité des composants et de l'environnement du système, il est essentiel de préserver toutes les preuves.

Visa recommande fortement de prendre les mesures suivantes :

7.1.1. Ne pas accéder aux systèmes compromis ni les modifier (p. ex. ne pas ouvrir de session ni changer les mots de passe ; ne pas se connecter avec des informations d'identification administratives). Les systèmes compromis doivent être mis hors ligne immédiatement et ne doivent pas être utilisés pour traiter des paiements ou établir une interface avec les systèmes de traitement des paiements.

7.1.2. Ne pas éteindre, redémarrer ou réinitialiser les systèmes compromis. Il convient plutôt de les isoler du reste du réseau en débranchant le ou les câbles réseau ou par d'autres moyens.

7.1.3. Identifier et documenter tous les composants suspectés d'être compromis (par exemple, les PC, les serveurs, les terminaux, journaux, événements de sécurité, bases de données, superpositions PED, etc.).

7.1.4. Documenter les actions de limitation et de remédiation entreprises, y compris les dates et heures (de préférence en UTC), les personnes impliquées et les actions détaillées effectuées.

7.1.5. Conserver tous les éléments de preuve et les journaux (par exemple, les éléments de preuve originaux tels que des images légales des systèmes et des logiciels malveillants, les événements de sécurité, les journaux Web, les journaux de base de données, les journaux de pare-feu, etc.)

Exigences pour les membres Visa

Les *Règles fondamentales Visa et les règlements relatifs aux produits et services Visa* (Règles Visa disponibles sur Visa en ligne) et dans le présent document intitulé *Quoi faire en cas de compromission* exigent que toutes les institutions financières membres de Visa (c.-à-d. émetteurs et acquéreurs) doivent mener une enquête approfondie en cas de perte, de vol ou de compromission, soupçonnés ou confirmés, de l'information relative au compte Visa ou au titulaire de carte Visa impliquant leur propre réseau ou celui de leurs marchands, opérateurs de traitement, passerelles, agents, fournisseurs de services, vendeurs tiers, revendeurs, intégrateurs et toute autre entité, ainsi que d'autres participants au système de paiement qui exploitent un environnement de paiement ou y accèdent.

1. Envoyer une notification à Visa

1.1. Dans les trois (3) jours civils suivant l'incident, signaler à l'équipe de gestion des risques de Visa tout accès non autorisé, soupçonné ou confirmé, aux données des titulaires de carte Visa.

Cette notification doit être adressée au bureau régional de l'équipe de gestion des risques de Visa :

Amérique du Nord (AN)	USFraudControl@visa.com
Amérique latine et Caraïbes (ALC)	LACFraudInvestigations@visa.com
Asie-Pacifique (AP) Europe centrale et orientale, Moyen-Orient et Afrique (ECMOA)	USFraudControl@visa.com
Assistance d'urgence 24/7 du Centre des opérations de gestion des risques	Numéro sans frais : 1 844-847-2106 International : 1 650-432-3379

Remarque : *Les acquéreurs Visa ayant accès à l'outil de gestion des enquêtes mondiales (GIMT) de Visa doivent fournir un avis par l'entremise du GIMT*

L'outil de gestion des enquêtes mondiales (GIMT) de Visa est une solution de gestion de cas de bout en bout qui sert de dépôt central pour la réception et la distribution de l'information d'enquête sur les événements de compromission et autres stratagèmes frauduleux. Les acquéreurs et leurs chargés du traitement de tiers (TPP) désignés sont tenus d'utiliser GIMT pour gérer les cas Visa. Pour plus de détails, veuillez vous référer au *Guide de l'acquéreur GIMT de Visa* sur Visa en ligne.

2. Effectuer une enquête initiale et fournir un rapport d'incident

2.1. Dans les trois (3) jours civils suivant la notification d'un événement de compromission soupçonné ou confirmé, fournir le rapport d'incident à Visa. Veuillez consulter l'annexe A à la fin du document pour obtenir une copie modifiable du rapport d'incident. Les membres de Visa sont tenus d'effectuer une enquête initiale et de soumettre un rapport d'incident au moyen de l'outil de gestion des enquêtes mondiales (GIMT) de Visa, tel que décrit à la section 1.

Ce rapport d'incident doit être adressé au bureau régional de l'équipe de gestion des risques de Visa :

Amérique du Nord (AN)	USFraudControl@visa.com
Amérique latine et Caraïbes (ALC)	LACFraudInvestigations@visa.com
Asie-Pacifique (AP) Europe centrale et orientale, Moyen-Orient et Afrique (ECMOA)	USFraudControl@visa.com
Assistance d'urgence 24/7 du Centre des opérations de gestion des risques	Numéro sans frais : 1 844-847-2106 International : 1 650-432-3379

Remarque : *Les acquéreurs Visa ayant accès à l'outil de gestion des enquêtes mondiales (GIMT) de Visa doivent fournir un avis par l'entremise du GIMT*

2.2. Le membre inscrit (c.-à-d. l'émetteur ou l'acquéreur) a la responsabilité de s'engager auprès de ses marchands, de ses opérateurs de traitement, de ses passerelles, de ses agents, de ses fournisseurs de services, de ses vendeurs tiers, de ses revendeurs, de ses intégrateurs et de toute autre entité, ainsi que d'autres participants au système de paiement qui exploitent un environnement de paiement ou y accèdent en son nom, afin d'enquêter sur tout événement compromettant potentiel et de le régler entièrement. À moins qu'elles ne soient divulguées à un membre enregistré, toutes les communications officielles de Visa concernant un évènement compromettant potentiel seront adressées à l'acquéreur enregistré.

2.3. Dans les trois (3) jours civils suivant la notification d'un événement compromettant, fournir à Visa l'état de la conformité aux exigences de la norme PCI DSS ou, le cas échéant, de la norme de sécurité des données des demande de paiement (PA- DSS) et de sécurité du NIP PCI au moment de l'incident.

2.4. Les informations fournies dans le rapport d'incident aident Visa à comprendre l'environnement réseau de l'entité compromise, la portée et l'exposition potentielles de l'incident, et à contenir l'événement. La documentation doit inclure toutes les mesures prises pour contenir et remédier à la compromission des données du compte.

2.5. Une enquête préliminaire n'est pas la même chose qu'un rapport judiciaire préliminaire. Les informations relatives à un rapport judiciaire préliminaire sont présentées à la section 4 ci-dessous.

3. Fournir à Visa les données exposées sur les comptes de paiement

3.1. Dans les trois (3) jours civils suivant l'un des scénarios suivants : (a) la découverte de données de compte compromises ; (b) la date à laquelle Visa demande les numéros de compte; ou (c) la détection d'une fenêtre d'exposition, les institutions financières membres de Visa sont tenues de s'assurer que tous les numéros de compte Visa compromis (connus ou soupçonnés) sont fournis à l'équipe de gestion des risques de Visa par l'entremise de l'outil de gestion des enquêtes mondiales (GIMT) ou du système de gestion des comptes compromis (CAMS) de Visa.

3.2. Les données de compte compromises connues ou suspectées doivent être établies à partir des enregistrements de transactions d'autorisation et identifiées par le mode d'entrée du point de vente (PDV), le cas échéant (c'est-à-dire POS 90, POS 05, POS 01, etc.) et téléchargées par des fichiers séparés.

3.3. Les membres qui téléchargent des comptes à risque dans le GIMT ou le CAMS doivent inclure les informations suivantes :

- Nom de l'entité
- Fenêtre d'exposition
- Éléments de données à risque (p. ex. numéro de compte principal (PAN), piste 1 ou piste 2, CVV2, NIP, date d'expiration, etc.)
- Identifiant d'acquisition, identifiant d'émission ou Opérateur de traitement VSS (le cas échéant)
- Code de catégorie de commerçant (MCC) (le cas échéant)
- Nom de l'enquêteur de l'organisme d'application de la loi et numéro d'incident (le cas échéant)
- Nom de l'enquêteur
- Numéro d'incident (le cas échéant)

3.4. Tous les fichiers doivent répondre aux critères suivants :

- Les fichiers doivent être en texte clair.
- La taille des fichiers ne doit pas dépasser 100 Mo.
- Le fichier téléchargé doit contenir uniquement des numéros de compte de 11 à 19 chiffres.

3.5. Si la date d'expiration est requise :

- La case pour la date d'expiration doit être cochée.
- Le format de la date doit être en AAMM.

Pour plus de détails, veuillez vous référer au *Guide de l'acquéreur GIMT de Visa* sur Visa en ligne.

4. Gérer l'enquête judiciaire PCI

4.1. Visa peut demander, à sa discrétion, à une entité compromise de faire appel à un enquêteur judiciaire PCI pour mener une enquête judiciaire indépendante. L'enquête doit être effectuée par un enquêteur judiciaire et les éléments suivants sont requis :

4.2. Les circonstances impliquant des entités à haut risque, qui comprennent, sans s'y limiter, les marchands de niveau 1 et 2, les opérateurs de traitement, les passerelles, les agents, les fournisseurs de services, les vendeurs tiers, les intégrateurs, les revendeurs ainsi que d'autres participants au système de paiement opérant ou accédant à distance à un environnement de paiement, présentent un risque inhérent plus élevé pour l'écosystème de paiement et peuvent nécessiter le recours à un enquêteur judiciaire PCI. Outre les entités à risque élevé, les facteurs suivants, entre autres, peuvent amener Visa à demander à une entité de mener une enquête PCI :

4.2.1. Perte pour cause de fraude liée aux rapports concernant les points d'achat communs.

4.2.2. Événement de compromission de données auto-déclaré pouvant affecter les informations d'identification de paiement.

4.2.3. Plusieurs sources, dont un organisme d'application de la loi, signalant que l'entité est potentiellement compromise.

4.2.4. Connexions malveillantes et nuisibles aux systèmes ou plateformes de paiement, y compris, mais sans s'y limiter, aux passerelles des opérateurs de traitement, aux systèmes de compensation et de règlement, etc.

4.2.5. Incapacité à contenir l'événement compromettant initial ou un événement compromettant antérieur (ceci peut être déterminé par des rapports relatifs aux points d'achat en commun supplémentaires, une analyse des données ou d'autres moyens).

4.3. S'il est informé qu'une enquête judiciaire est nécessaire, le membre est tenu d'engager ses marchands, processeurs, passerelles, agents, fournisseurs de services, vendeurs tiers, revendeurs et intégrateurs afin d'enquêter sur tout événement de compromission potentiel et d'y remédier pleinement.

4.3.1. Dans les cinq (5) jours ouvrables, signer un contrat pour retenir les services d'un enquêteur judiciaire pour effectuer une enquête PCI et informer Visa de l'organisation judiciaire et de l'enquêteur principal. Visa n'acceptera PAS les rapports judiciaires provenant d'organisations non approuvées

4.3.2. Dans les cinq (5) jours ouvrables suivant l'exécution du contrat, fournir à Visa le rapport initial (c'est-à-dire préliminaire).

4.3.3. Dans les dix (10) jours ouvrables suivant la fin de l'enquête judiciaire, fournir à Visa un rapport judiciaire final.

4.3.4. Fournir un soutien logistique et technique complet à l'enquêteur pour faciliter l'achèvement rapide de l'enquête, y compris, mais sans s'y limiter, des mises à jour régulières de l'état d'avancement, la participation à des conférences téléphoniques avec toutes les parties, la fourniture d'échantillons de logiciels malveillants et d'indicateurs de compromission, etc.

4.3.5. L'enquêteur ne peut provenir d'une société qui est affiliée à l'entité compromise ou qui a fourni des services à l'entité compromise, comme enquête précédente de l'enquêteur, un évaluateur de sécurité qualifié (QSA), un conseiller, un consultant, une surveillance ou un support de sécurité réseau, au cours des 3 dernières années.

4.3.6. Les enquêteurs judiciaires sont tenus de communiquer tous les rapports d'enquête judiciaire PCI et leurs conclusions directement à Visa. Les enquêteurs judiciaires sont tenus de communiquer à Visa, au membre et à l'entité compromise toutes les divergences ou les questions en suspens avant de finaliser le rapport. Visa se réserve le droit de rejeter un rapport judiciaire s'il ne répond pas aux exigences établies dans le Guide du programme de l'enquêteur judiciaire PCI ou s'il ne répond pas aux exigences du présent document. Le non-respect des exigences relatives aux enquêtes judiciaires précisées ci-dessus peut entraîner des évaluations de non-conformité.

4.3.7. Visa se réserve le droit d'exiger des enquêtes judiciaires supplémentaires ou d'engager directement un enquêteur judiciaire pour effectuer des enquêtes judiciaires supplémentaires, si, à sa seule discrétion, elle détermine que les exigences du présent document n'ont pas été satisfaites. Toute enquête judiciaire supplémentaire sera aux frais du membre. Ces frais s'ajoutent à toute évaluation de non-conformité.

4.4. 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 SSC, qui est accessible sur le site : www.pcisecuritystandards.org/document_library (Filtré par : PFI)

Liste des enquêteurs judiciaires PCI approuvés :

https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

4.5. À la suite de l'enquête, toutes les entités compromises, y compris, mais sans s'y limiter, toutes les institutions financières membres de Visa (c.-à-d. les émetteurs et les acquéreurs), les marchands, les opérateurs de traitement, les passerelles, les agents, les fournisseurs de services, les vendeurs tiers, les intégrateurs et revendeurs et toute autre entité, ainsi que les autres participants au système de paiement qui exploitent un environnement de paiement ou y accèdent, sont tenus de prendre les mesures suivantes : Une conformité PCI entière avec les normes PCI DSS, PCI PA-DSS et, le cas échéant, la validation de la conformité aux exigences de sécurité du NIP PCI selon les *Règles Visa*.

Veuillez visiter le www.pcisecuritystandards.org pour plus d'informations sur la PCI DSS et les exigences en matière de sécurité du NIP PCI.

5. Gérer l'enquête indépendante

5.1. Ce ne sont pas tous les cas de compromission qui nécessitent une enquête judiciaire. Visa peut exiger qu'une entité potentiellement compromise mène une enquête indépendante au lieu de, ou avant, une enquête judiciaire PCI. Si elle est informée qu'une enquête indépendante est nécessaire, une entité est tenue de faire ce qui suit :

5.1.1. Dans les cinq (5) jours ouvrables, signer un contrat pour retenir les services d'un enquêteur pour effectuer une enquête indépendante et fournir à Visa le nom de la société judiciaire et de l'enquêteur principal.

5.1.2. Dans les cinq (5) jours ouvrables suivant l'exécution du contrat, fournir à Visa le rapport initial (c'est-à-dire préliminaire).

5.1.3. Dans les dix (10) jours ouvrables suivant la fin de l'enquête, fournir à Visa un rapport final.

5.1.4. Fournir un soutien logistique et technique complet à l'enquêteur pour faciliter l'achèvement rapide de l'enquête, y compris, mais sans s'y limiter, des mises à jour régulières de l'état d'avancement, la participation à des conférences téléphoniques avec toutes les parties, la fourniture d'échantillons de logiciels malveillants et d'indicateurs de compromission, etc.

5.2. L'enquêteur ne peut provenir d'une société qui est affiliée à l'entité compromise ou qui a fourni des services à l'entité compromise, comme une enquête précédente de l'enquêteur, un évaluateur de sécurité qualifié (QSA), un conseiller, un consultant, une surveillance ou un support de sécurité réseau, au cours des 3 dernières années.

5.3. Les enquêteurs sont tenus de fournir les rapports et les résultats de leurs enquêtes directement à Visa.

5.4. Visa se réserve le droit de rejeter les rapports qui ne satisfont pas aux exigences du présent document.

5.5. Visa se réserve le droit d'exiger une enquête judiciaire si l'enquête indépendante ne satisfait pas aux exigences du présent document.

6. Exigences spécifiques pour un événement compromettant suspecté ou confirmé pour les membres

6.1. Visa a observé une augmentation des attaques contre les institutions financières membres. Toute institution financière membre qui soupçonne ou confirme un accès non autorisé aux données des titulaires de la carte Visa, y compris les systèmes de paiement qui stockent, traitent ou transmettent les données des titulaires de carte, doit se conformer aux exigences décrites dans la présente section.

6.1.1. Visa peut exiger d'un membre qu'il fasse appel à un enquêteur judiciaire et fournisse les mêmes éléments que ceux décrits à la section 4.

6.1.2. Ce ne sont pas tous les cas qui nécessitent une enquête judiciaire. Visa peut exiger ce qui suit au lieu ou avant une enquête judiciaire PCI. Ces mesures doivent être appliquées dans un délai de (3) jours civils :

- Si Visa avise le membre de l'existence de connexions de protocoles Internet (IP) malveillantes, le membre est tenu de confirmer qu'un pare-feu est en place pour les connexions sortantes.
- Le membre doit vérifier les journaux du réseau pour savoir quelles machines se sont connectées à des adresses IP malveillantes et fournir l'accès aux journaux, sur demande.
- Le membre est tenu de balayer son réseau à la recherche d'activités suspectes et d'effectuer une enquête supplémentaire sur toute machine observée communiquant avec des adresses IP malveillantes. Visa peut demander des indicateurs de compromission, par exemple des fichiers malveillants, y compris des échantillons de logiciels malveillants, pour appuyer l'enquête.
- Le membre est tenu de documenter les mesures susmentionnées et de fournir un rapport d'incident à Visa.
- Pendant l'enquête, le membre est tenu de surveiller et de signaler toute activité suspecte ou frauduleuse sur tout autre système de paiement qu'il exploite, y compris, mais sans s'y limiter, les services SWIFT, ACH, B2B et P2P.
- Visa recommande fortement qu'un tiers indépendant valide la sécurité du réseau du membre. Dans certains cas, Visa peut exiger une validation par un tiers afin de confirmer que le réseau du membre est sécuritaire.

Interruption de la menace liée au commerce électronique de Visa (eTD)

La perturbation de la menace liée au commerce électronique (eTD) de Visa est une nouvelle fonction exclusive qui permet à Visa de détecter et de neutraliser les événements frauduleux liés au commerce électronique des commerçants avant que la fraude ne soit signalée. eTD utilise une technologie et des techniques d'enquête sophistiquées pour identifier de façon proactive les événements frauduleux liés au commerce électronique, fournir des conseils sur la suppression des logiciels malveillants et limiter l'exposition des données des cartes de paiement.

La fonction eTD de Visa s'efforce de réduire le risque et de stopper la fraude liée aux événements compromettants du commerce électronique. Il s'agit d'une fonction de portée mondiale et d'un service à valeur ajoutée de Visa qui vise à protéger l'écosystème des paiements. eTD est disponible pour tous les commerçants de commerce électronique qui acceptent Visa.

7. Exigences eTD pour les membres Visa

7.1. Lorsqu'un membre est avisé qu'un cybermarchand a été identifié comme compromis par l'intermédiaire d'eTD, le membre est tenu de prendre les mesures suivantes :

Enquête initiale

7.1.1. Dans les trois (3) jours ouvrables suivant la réception d'une notification eTD, effectuer une enquête initiale avec le marchand identifié et fournir le rapport d'incident à Visa via GIMT. Le rapport doit documenter les conclusions et toute mesure prise pour contenir l'incident. Veuillez vous reporter à l'annexe A à la fin du document pour obtenir une copie modifiable du rapport d'incident.

7.1.2. Ces informations permettront à Visa de comprendre l'exposition potentielle et d'aider à contenir l'incident.

Limitation et résolution de l'événement compromettant

7.1.3. Dans les vingt (20) jours ouvrables suivant la réception d'une notification eTD, s'assurer que l'événement de compromission est contenu et corrigé.

7.1.4. Les membres doivent travailler avec le cybermarchand pour s'assurer que ce dernier valide la conformité PCI DSS.

Enquête judiciaire PCI

7.1.5. Si l'événement de compromission n'est pas contenu et résolu dans les vingt (20) jours ouvrables, Visa peut exiger une enquête judiciaire PCI de l'entité et des évaluations de non-conformité. Les frais d'enquête et les évaluations de non-conformité sont imputés au membre.

7.1.6. Visa se réserve le droit d'accélérer les échéances susmentionnées afin d'être conforme aux exigences décrites dans la section 4, Gérer l'enquête judiciaire PCI, du présent document.

Frais d'enquête et évaluations de non-conformité

8. Frais d'enquête

(En vigueur depuis le 18 avril 2020 dans les régions AP, ECMOA, ALC, et aux É-U.)
(En vigueur depuis le 18 juillet 2020 au Canada)

Visa s'engage à promouvoir la prospérité sûre et solide à long terme du système de paiement Visa et continue de faire des investissements importants dans la technologie des paiements afin de protéger le système de paiement. À cette fin, Visa vise à assurer la résolution opportune des événements compromettants et à promouvoir la notification des comptes à risque afin d'endiguer les impacts de la fraude. Pour atteindre ces objectifs, Visa a élaboré des frais d'enquête pour inciter les entités à coopérer pleinement avec Visa à chaque étape du processus d'enquête et à terminer l'enquête en temps opportun. La pleine coopération au cours d'une enquête aide à contenir et à résoudre rapidement un événement compromettant et à minimiser la fraude qui en résulte pour les clients de Visa.

Les frais d'enquête ne s'appliquent qu'aux enquêtes dirigées par une organisation judiciaire. Si une enquête judiciaire PCI n'est pas terminée dans les 4 (quatre) mois civils complets à partir de la date à laquelle Visa a fourni un avis de l'exigence d'une enquête judiciaire, Visa peut imposer des frais comme suit :

8.1. Des frais fixes d'un montant de 3 000 dollars américains pour les enquêtes concernant les commerçants de niveau 3 et 4, ou

8.2. Des frais mensuels récurrents d'un montant de 10 000 dollars américains pour les enquêtes concernant les commerçants de niveaux 1 et 2, les opérateurs de traitement VisaNet, les membres et les agents, jusqu'à ce que l'enquête soit dûment terminée.

La période de 4 mois commence le 1er du mois suivant la réception par le membre d'un avis de Visa selon lequel une enquête judiciaire PCI est requise. Les mois partiels ne sont pas inclus dans la période de quatre mois sans frais ni dans le calcul des frais.

Les frais seront facturés après le 5e mois civil complet d'une enquête ouverte.

Entité	Nombre de transactions annuelles	Durée de l'enquête — Période de grâce	Durée de l'enquête — Période de frais	Frais d'enquête
Émetteurs	S.O.	Quatre mois civils complets (les mois partiels ne sont pas inclus)	Les frais mensuels commencent au cinquième mois civil complet et se poursuivent pendant chaque mois civil complet jusqu'à ce que l'enquête soit terminée.	10 000 dollars américains par mois
Acquéreurs	S.O.			
Opérateur de traitement VisaNet	S.O.			
Niveau 1 — Marchands	> 6 000 000			
Niveau 1 — Agents pour émetteurs ou acquéreurs	> 300 000			
Niveau 2 — Marchands	1 000 001 à 6 000 000			
Niveau 2 — Agents pour émetteurs ou acquéreurs	< 300 000			
Niveau 3 — Cybermarchands	20 000 à 1 000 000	Quatre mois civils complets (les mois partiels ne sont pas inclus)	Frais uniques à partir du cinquième mois complet	3 000 dollars américains frais fixes
Niveau 4 — Marchands	1 à 1 000 000			

9. Évaluation de non-conformité

(En vigueur depuis le 18 avril 2020 dans les régions AP, ECMOA, ALC, et aux É-U.)
(En vigueur depuis le 18 juillet 2020 au Canada)

Un membre est assujetti à une évaluation de non-conformité de 100 000 dollars américains par incident s'il ne respecte pas l'une des exigences ci-dessous :

- Dans les trois (3) jours civils suivant l'incident, signaler à l'équipe de gestion des risques de Visa tout accès non autorisé, soupçonné ou confirmé, aux données des titulaires de carte la Visa ou au système de paiement.
- Fournir à Visa l'état de la conformité à la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) et, le cas échéant, à la norme de sécurité des données des demandes de paiement (PA-DSS) et aux exigences de sécurité du NIP de l'industrie des cartes de paiement (PCI) dans les trois (3) jours civils suivant l'incident.
- Dans les trois (3) jours civils suivants le constat, les membres sont tenus d'effectuer une enquête initiale et de fournir à Visa le rapport d'incident documentant les constatations ou les conclusions.
- Dans les trois (3) jours civils suivant l'un des scénarios suivants : (a) la découverte de données de compte compromises ; (b) la date à laquelle Visa demande les numéros de compte; ou (c) la détection d'une fenêtre d'exposition, les institutions financières membres de Visa sont tenues de s'assurer que tous les numéros de compte Visa compromis (connus ou soupçonnés) sont fournis à l'équipe de gestion des risques de Visa par l'entremise de l'outil de gestion des enquêtes mondiales (GIMT) ou du système de gestion des comptes compromis (CAMS) de Visa.

- Engager un enquêteur judiciaire PCI approuvé dans les cinq (5) jours ouvrables suivant la notification d'un événement de compromission soupçonné ou confirmé, si Visa le demande.
- Dans les cinq (5) jours ouvrables, signer un contrat pour retenir les services d'un enquêteur judiciaire pour effectuer une enquête PCI et informer Visa de l'organisation judiciaire et du nom de l'enquêteur principal, tel que décrit dans la section 4.
- Dans les cinq (5) jours ouvrables suivant l'exécution du contrat, fournir à Visa le rapport initial (c'est-à-dire préliminaire).
- Dans les dix (10) jours ouvrables suivant la fin de l'enquête judiciaire, fournir à Visa un rapport judiciaire final.
- Fournir un soutien logistique et technique complet à l'enquêteur judiciaire afin de faciliter la réalisation de l'enquête en temps opportun.
- Engager un enquêteur judiciaire PCI approuvé dans les cinq (5) jours ouvrables suivant la notification d'un événement de compromission soupçonné ou confirmé, si Visa le demande, tel que décrit dans la section 5.
- Dans les cinq (5) jours ouvrables, signer un contrat pour retenir les services d'un enquêteur pour effectuer une enquête indépendante et fournir à Visa le nom de la société judiciaire et de l'enquêteur principal.
- Dans les cinq (5) jours ouvrables suivant l'exécution du contrat, fournir à Visa le rapport initial (c'est-à-dire préliminaire).
- Dans les dix (10) jours ouvrables suivant la fin de l'enquête, fournir à Visa un rapport final.
- Fournir un soutien logistique et technique complet à l'enquêteur indépendant afin de faciliter la réalisation de l'enquête en temps opportun.
- Dans les vingt (20) jours ouvrables suivants la réception d'une notification TD, les membres sont tenus de s'assurer que les risques sont contenus et neutralisés.

Annexe Q : Rapport d'incident

Page 1 du rapport d'incident Visa				
Nom de l'entité juridique :				
Nom de l'entité DBA :				
Type de l'entité : *(c.-à-d. : membre FI, marchand, agent, fournisseur de services, revendeurs etc.)*				
Services, solutions ou produits fournis par l'entité :				
Adresse de l'entité :	Ville :	État/Province :	Code postal :	Pays :
Nom de la personne-ressource principale :	Téléphone :		Courriel :	

Toutes les informations ci-dessous doivent être fournies par l'entité ou l'équipe de réponse aux incidents.
Description détaillée de l'incident (quoi, comment, qui, quand et où) : *Remarque : Si l'incident touche plusieurs emplacements ou entités, veuillez fournir une liste des noms, des adresses, des banques marchandes et des opérateurs de traitement des marchands ou des entités touchées :*
Énumérez la ou les fenêtres d'intrusion et d'exposition :
Énumérer les éléments de données exposés *(p. ex., numéro de compte, date d'expiration, nom du titulaire de carte, CVV, CVV2, adresse, courriel, etc.)* Si des données sur les comptes ont été compromises, indiquez le nombre de comptes Visa touchés :
Détaillez toutes les mesures prises pour enquêter sur l'incident suspecté ou confirmé (quoi, comment, qui, quand et où), y compris leur chronologie :
Avez-vous fait appel à l'expertise de tiers dans cette affaire ? ☐ Oui ☐ Non Si oui, veuillez les énumérer et décrire leur rôle :
Quel type de solution d'accès à distance est utilisé ?
L'authentification à deux facteurs est-elle utilisée pour l'accès à distance ? ☐ Oui ☐ Non
L'entité a-t-elle reçu des plaintes concernant des transactions frauduleuses de la part de ses clients ? ☐ Oui ☐ No Si oui, veuillez les décrire :

Page 2 du rapport d'incident Visa

L'entité a-t-elle été contactée par un organisme d'application de la loi ? ☐ Oui ☐ Non
Si oui, indiquez la ou les dates, l'organisme chargé de l'application de la loi et la raison de ce contact : *(par exemple, suspicion d'un événement compromettant pour l'entité, plaintes frauduleuses de clients de l'entité, etc.)*

L'entité a-t-elle contacté un organisme chargé de l'application de la loi au sujet de l'incident ? Si oui, indiquez la ou les dates et le nom de l'organisme chargé de l'application de la loi. ☐ Oui ☐ Non

Est-ce que l'incident a été contenu ? ☐ Oui ☐ Non
Si oui, comment et quand ?

Si vous êtes un marchand, veuillez fournir les renseignements suivants :

ID marchand :	CC :	Niveau PCI DSS :	Volume annuel de transactions :	Société ou franchisé :	# d'emplacement :

Conformité PCI ☐ Oui ☐ Non Dernière date de validation de la norme PCI DSS :

Identifiant d'acquéreur, identifiant d'émetteur, ou opérateur de traitement VSS : (Énumérez tous les éléments applicables) :

Opérateur(s) de traitement :	Information de contact sur l'opérateur de traitement :

L'appareil de point de vente (PDV) est-il conforme à la norme EMV ? ☐ Oui ☐ Non

La solution de point de vente permet-elle un cryptage de bout en bout ? ☐ Oui ☐ Non

Le site de commerce électronique est-il hébergé ? ☐ Oui ☐ Non
Si oui, veuillez indiquer le nom et les coordonnées de la personne à contacter :

Identifier la ou les parties responsables de la configuration et du soutien de la solution de point de vente (PDV) *(c.-à-d. : QIR, revendeur, ou agent).*	NOM	TITRE	COORDONNÉES
	(Si l'entité est un intégrateur ou un revendeur, veuillez joindre une liste de tous les identifiants d'acquéreurs et de tous les noms des marchands, des cartes de marchands, des identifiants d'accepteurs, la ville et la province).		

Rapport rédigé par :

Nom	Titre	Rôle

Courriel	Téléphone	Date d'achèvement