L'avenir de la sécurité des paiements au Canada

Octobre 2017

Avis

Énoncés prospectifs

Cette présentation contient des énoncés prospectifs au sens de la Private Securities Litigation Reform Act de 1995 des États-Unis. Vous pouvez reconnaître ces énoncés par l'emploi des termes « objectif », « but », « stratégie », « occasions », « continuer », « peut » et du futur, ainsi que d'autres références semblables à l'avenir. Les exemples de tels énoncés prospectifs peuvent comprendre, sans toutefois s'y limiter, les énoncés que nous formulons concernant notre stratégie d'entreprise et nos buts, plans et objectifs en matière de produits. De par leur nature, les énoncés prospectifs : (i) ne sont valables que pour la date à laquelle ils sont formulés, (ii) ne sont ni des énoncés de faits historiques ni des garanties de rendement futur et (iii) sont assujettis à des risques, des incertitudes, des hypothèses et des changements dans les circonstances qui sont difficiles à prédire ou à quantifier. Ces énoncés prospectifs sont basés sur nos hypothèses, nos attentes et nos projections actuelles concernant les événements futurs qui reflètent le meilleur jugement de la direction et qui comportent un certain nombre de risques et d'incertitudes qui pourraient faire en sorte que les résultats réels diffèrent considérablement des résultats suggérés par nos commentaires aujourd'hui. Donc, les résultats réels peuvent différer considérablement et négativement des énoncés prospectifs en raison de divers facteurs. Vous devriez examiner et prendre en considération les renseignements contenus dans nos documents déposés auprès de la SEC concernant ces risques et ces incertitudes. Vous ne devriez pas vous fier indûment à de tels énoncés. À moins que la loi ne l'exige, nous n'avons pas l'intention de mettre à jour ou de réviser tout énoncé prospectif en raison de nouveaux renseignements ou de faits nouveaux futurs, ou autrement.

Avis sur les marques de tiers

Toutes les marques et tous les logos de tiers utilisés dans cette présentation appartiennent à leurs propriétaires et sont utilisés aux fins d'identification seulement, sans en faire la promotion.

Droit d'auteur

Situation actuelle de la fraude

Situation actuelle de la fraude

Depuis plus de 60 ans, Visa collabore avec l'industrie pour diminuer les cas de fraude et les maintenir au minimum. La technologie a beaucoup contribué à cette baisse, allant des autorisations en ligne jusqu'à l'adoption mondiale de la technologie de la carte à puce. Bien que les taux de fraude demeurent marginaux – environ sept cents par tranche de 100 $ de transactions[1] – on commence à constater l'incidence des données compromises. Le taux de fraude à l'échelle mondiale continue de se réorienter vers le réseau sans présence de la carte (SPC), soit la fraude perpétrée sur les opérations effectuées en ligne ou par téléphone.

Entre 2006 et 2016, les fraudes SPC sur VisaNet sont passées de 35 % à 57 %[2].

En quoi consiste 3D Secure?

3DS est un protocole mondial du secteur qui procure un mécanisme d'authentification du titulaire de carte au moment d'un achat électronique.

Le marché canadien n'en est pas épargné :

Les fraudes sans présence de la carte représentaient 78 % de toutes les fraudes perpétrées relativement aux comptes canadiens la fin du mois de mars 2017[4].

60 % des pertes dues aux fraudes sans la présence de carte liées aux comptes canadiens se sont produites à l'extérieur du Canada à la fin du mois de mars 2017[1].

74 % des pertes dues aux fraudes chez les marchands canadiens étaient commises dans le réseau SPC pendant le mois se terminant en mars 2017[1].

Plus de 97 % des fraudes sans présence de la carte se produisent lorsque le mécanisme d'authentification renforcée 3D Secure (3 Domain Secure) n'est pas activé[3].

La fraude par carte falsifiée est la moins perpétrée pour les comptes Visa au Canada, représentant 11 % des pertes en dollars; ce chiffre diminue chaque année grâce à la mise en œuvre réussie de la technologie de la carte à puce EMV pour les cartes et terminaux au Canada[1].

La fraude par carte falsifiée transfrontalière, soit les cas où des cartes émises au Canada sont utilisées hors du Canada siminue aussi grâce à l'adoption des terminaux EMV connue aux États-Unis[1].

[1] Source : Rapport sur la fraude Visa (TC40) et ventes, septembre 2017
[2] Source : Données de règlement de VisaNet, décembre 2016
[3] Source : Volume commercial électronique de Visa et tableau de bord de Rapports d'entreprise Visa, 6 juin 2017
[4] Source : Données de référence sur le rendement en matière de fraude. Rapport TC40 sur la fraude signalée par les émetteurs et données de règlement de VisaNet, 2017

Situation actuelle de la fraude

Au cours des dix-huit derniers mois, Visa a mis sur pied un groupe de travail multifonctionnel composé de clients et d'intervenants de l'industrie afin d'aider à communiquer les principaux éléments de notre feuille de route en tenant compte de nos objectifs communs qui visent à freiner la croissance des fraudes sans présence de la carte et la sécurisation des données. À l'issue de cette consultation, il a été décidé que les éléments suivants seront progressivement éliminés au fil du temps.

	Sécurité des données		Prévention de la fraude	
Piliers stratégiques	Dévaluation	Protection	Exploitation	Habilitation
	• Aucune transaction de rechange par bande magnétique • Point de vente qui accepte la puce EMV à 100 % • Segmentation en unités	• PCI DSS version 3.2	• Authentification dynamique basée sur le risque (3DS 2.0) • Utilisation élargie de la CVV2 • Amélioration du processus d'autorisation	• Alertes pour les consommateurs • Registre mondial des fournisseurs de services

1. Dévaluation des données

1. Dévaluation des données

Aucune transaction de rechange par bande magnétique ne se fera à un point de vente qui accepte les cartes à puce EMV

Situation actuelle

Une transaction de rechange se produit lorsqu'une carte à puce utilisée dans un terminal de carte à puce ne peut pas être lue à cause d'un problème technique lié à la puce ou au terminal. Lorsque la puce ne peut pas être lue, la technologie procède à une transaction de « rechange » par bande magnétique. Cela arrive peu souvent, car les puces EMV sur les cartes sont rarement défectueuses. Le taux de fraude pour les transactions de rechange par bande magnétique est nettement supérieur à celui des transactions par puce[1].

[1]Source : TC40 rapport de fraude et données de règlement du quatrième trimestre 2016

L'avenir

Pour mieux protéger les transactions en présence de la carte, Visa procède actuellement à des changements en vertu desquels les marchands seront tenus de refuser les transactions par carte à puce qui sont traitées comme des transactions par bande magnétique dans un terminal de carte à puce.

Exigences

À compter du 14 avril 2018, si une carte à puce EMV ne fonctionne pas correctement chez un marchand utilisant un lecteur de carte à puce et que ce marchand tente de traiter la transaction en glissant la bande magnétique, l'émetteur doit refuser la transaction.

1. Dévaluation des données

Point de vente (PDV) qui accepte la puce EMV à 100 %

Situation actuelle

L'introduction de la technologie de la carte à puce (EMV) améliorée a ouvert la voie aux innovations, notamment les paiements sans contact et mobiles. Les cartes à puce génèrent un code unique chaque fois qu'elles sont utilisées en magasin à un terminal activé par une puce. Contrairement aux cartes à bande magnétique, il est pratiquement impossible de reproduire ces cartes, empêchant ainsi les fraudes en magasin.

Afin de protéger davantage l'écosystème, Visa a introduit la politique de transfert de responsabilité au mois de mars 2011. Cette politique encourage les marchands à accepter les transactions effectuées avec une carte à puce, les astreignant à assumer la responsabilité des fraudes par cartes contrefaites s'ils décidaient de ne pas accepter cette forme de paiement.

Au Canada, près de 93 %[1] des transactions sont effectuées avec la présence d'une carte à puce. Un petit nombre de marchands n'ont pas encore adopté les terminaux qui utilisent la technologie de carte à puce, exposant ainsi les consommateurs à des risques.

[1] Source : Tableau de bord de suivi de l'implantation de l'authentification (de mai à juillet 2017)

L'avenir

Nous croyons que protéger les marchands contre les pertes est une saine pratique commerciale. Par conséquent, nous avons l'intention d'éliminer les transactions effectuées avec une carte à bande magnétique au profit de terminaux, guichets automatiques et comptes émis au Canada qui peuvent tous prendre en charge des cartes EMV.

Politique Responsabilité zéro Visa

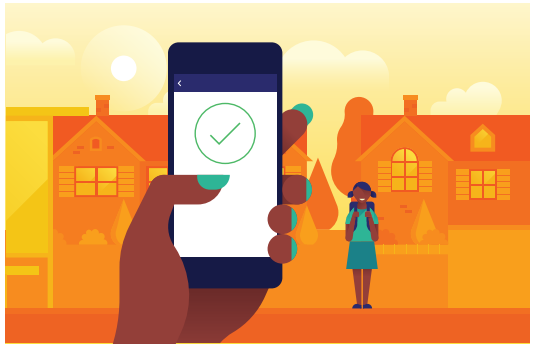
Toutes les transactions effectuées aujourd'hui avec la carte Visa, avec ou sans puce, sont sécurisées grâce à la Politique Responsabilité zéro de Visa qui protège les titulaires de carte Visa de toute responsabilité en cas de fraude.

Exigences

À compter du 14 octobre 2020, tous les marchands devront pouvoir traiter les cartes à puce EMV, à l'exception de ceux munis de terminaux qui acceptent les demandes de titulaires de carte sans aide. Ces marchands devront pouvoir traiter les cartes à puce EMV à compter du 14 octobre 2022.

1. Dévaluation des données

Segmentation en unités



Renseignements au dossier

La croissance du commerce numérique et l'émergence des nouveaux modèles d'affaires ont augmenté le nombre de transactions où les renseignements de paiement des titulaires (par ex. le numéro du compte ou du jeton) sont conservés au dossier du marchand, du fournisseur du portefeuille numérique ou autre fournisseur de services, afin qu'ils puissent être utilisés sans heurts lors de transactions futures.

Situation actuelle

En 2013, Visa a dirigé une collaboration mondiale sur la segmentation en unités et joué un rôle important dans l'élaboration des normes qui régissent la segmentation EMVCo. La segmentation en unités est une initiative coordonnée par l'ensemble de l'industrie qui ajoute une couverture supplémentaire de sécurité pour les paiements mobiles et numériques afin de prévenir la fraude entre les réseaux en réduisant les conflits lors de l'expérience de magasinage.

Elle vise à offrir une compatibilité et limiter les changements apportés à l'écosystème. L'objectif en matière de sécurité pour tout processus de segmentation en unités consiste à remplacer les renseignements du titulaire du compte, notamment les numéros de compte et les dates d'expiration au moyen d'un identificateur numérique unique (un « jeton »). Ce jeton peut être unique à l'appareil, au fournisseur du portefeuille ou à l'étui d'utilisation, tout comme des renseignements au dossier.

L'avenir

Le service de jetons Visa utilise les exigences de la segmentation EMVCo pour fournir un service aux émetteurs, acquéreurs, marchands et traiteurs des cartes Visa afin qu'ils puissent mettre en œuvre des services de segmentation en unités en réseau pour les comptes Visa. À l'heure actuelle, le service de jetons prend en charge les portefeuilles de l'émetteur et tiers comme Apple Pay[MC], Samsung Pay[MC] et Android Pay[MC].

Les jetons constitueront un outil essentiel en ce qui a trait aux paiements intégrés des appareils et dispositifs prêts-à-porter de l'Internet des objets (IdO), comme Garmin Pay[MC].

2. Protection des données sensibles

2. Protection des données sensibles

PCI DSS Version 3.2

Situation actuelle

La conformité au PCI DSS est le fondement même des programmes de conformité et de sécurité des données de Visa et elle se veut un élément essentiel de la protection des données sensibles du titulaire de carte contre les compromis. PCI DSS établit les exigences techniques et opérationnelles afin d'aider les organisations (marchands, institutions financières, fournisseurs de traitement de paiement, fournisseurs de services et de technologies) à se protéger des cyberattaques qui tentent de voler les données du titulaire.

L'avenir

Le Conseil des normes de sécurité PCI (PCI SSC) a publié de nouvelles normes en matière de sécurité des données au mois d'avril 2016 : PCI DSS version 3.2 (de la version 3.1) afin de répondre aux menaces croissantes de vol des renseignements de paiement des clients. Les entreprises qui acceptent, traitent ou reçoivent des paiements devraient adopter la version 3.2 afin de prévenir, de détecter et de contrecarrer les cyberattaques qui aboutissent à des violations.

2. Protection des données sensibles

Données de la bande magnétique sans contact

Situation actuelle

La mise en œuvre hâtive de l'acceptation de la transaction sans contact tenait compte des terminaux qui acceptent les données de la bande magnétique sans contact. La majorité des terminaux sans contact au Canada acceptent désormais les transactions en lisant les données de la bande magnétique et des cartes de débit / crédit Visa Smart (qVSDC).

Une transaction effectuée sans contact signifie que le terminal lit la puce EMV sans contact, mais traite la transaction comme une transaction par bande magnétique.

À l'heure actuelle, les règles de Visa exigent que les terminaux déployés au Canada qui acceptent la carte sans contact respectent la norme des paiements sans contact de Visa et puissent être en mesure de traiter des transactions des deux façons.

L'avenir

On a signalé à Visa une activité frauduleuse où des criminels avaient simulé des transactions sans contact.
Les fraudeurs utilisent une application mobile qui imite les transactions par bande magnétique sans contact de Visa chez un marchand qui accepte les cartes sans contact.

Afin de contrecarrer ce risque, les dispositifs qui acceptent les cartes sans contact au Canada ne pourront plus prendre en charge les transactions par la lecture des données par bande magnétique.

Exigences

À compter du 19 octobre 2019, tous les dispositifs qui acceptent les cartes sans contact au Canada ne pourront plus prendre en charge les transactions par la lecture des données par bande magnétique.

3. Exploitation des données

3. Exploitation des données

Authentification dynamique basée sur le risque (3DS 2.0)

Situation actuelle

Le service 3DS est un protocole de messagerie qui permet aux consommateurs d'authentifier directement leur compte auprès de l'émetteur du compte lors des achats en ligne.

À l'heure actuelle, 3DS est peu accepté par les marchands (environ 3,8 %[1] l'utilisaient en date de juillet 2017) en raison de conflits causés aux consommateurs et des conséquences de ces conflits sur l'abandon du panier d'achats chez les marchands.

Les émetteurs canadiens ont entamé la migration du mot de passe spécifique exigé par le protocole 3DS pour chaque transaction à un modèle d'authentification axée sur le risque. Au mois d'avril 2017, 62,2 %[2] des comptes associés aux émetteurs canadiens prenaient en charge l'authentification axée sur le risque.

[1] Source : Volume commercial électronique de Visa et tableau de bord de Rapports d'entreprise Visa, 6 juin 2017.
[2] Source : Donnés de règlement de Visa, août 2017

L'avenir

Vu la rétroaction que le secteur a donnée, EMVCo a lancé une nouvelle version du protocole 3DS (version 2.0) en octobre 2016. La nouvelle version procure une meilleure expérience d'utilisation, est compatible avec les applications mobiles, les appareils connectés et des données plus riches pour favoriser une prise de décision rigoureuse d'authentification fondée sur les risques. La majorité des transactions n'exigera aucune authentification par le titulaire de la carte. Dans le cas de certaines transactions, il se peut que les émetteurs exigent une authentification supplémentaire. Dans ces cas, le protocole 3DS 2.0 permet aux titulaires de cartes d'authentifier plus facilement leur identité en temps réel au moyen d'un mot de passe dynamique fourni par texte sur un téléphone mobile ou par un dispositif qui génère un mot de passe unique.

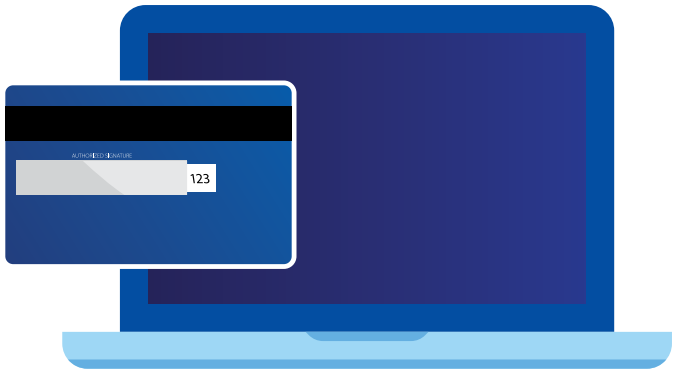
Exigences

À compter du 14 avril 2018, Visa éliminera l'utilisation de mots de passe statiques spécifiques au 3DS et les processus d'adhésion connexes.

Les marchands qui authentifient les transactions à l'aide de 3D-Secure sont généralement protégés contre les demandes de débit compensatoire de l'émetteur liées aux fraudes sans présence de la carte et cette règle vaudra pour toutes les tentatives de transactions par le marchand avec le protocole 3-D Secure 2.0 après le 12 avril 2019, la date d'activation du programme à l'échelle mondiale.

3. Exploitation des données

Élargir l'utilisation du code CVV2



Situation actuelle

Le code CVV2 (Valeur de vérification de la carte 2) est un nombre à trois chiffres imprimé au verso de la carte de crédit ou de débit, utilisé pour authentifier une transaction sans présence de la carte.

Le numéro CVV2 de la carte fourni à un marchand lui indique que vous avez la carte de crédit ou de débit avec vous, protégeant ainsi votre transaction tout en réduisant les fraudes.

L'avenir

Pour contribuer à réduire la fraude sans présence de la carte, Visa procède actuellement à des changements pour généraliser l'usage de la CVV2 aux marchands par téléphone ou par commerce électronique au Canada.

Le recours à la CVV2 protège les marchands qui effectuent des transactions sans présence de la carte contre la compromission des données du numéro de compte et de date d'expiration qui pourrait exister dans le réseau actuel de cartes, puisque la CVV2 ne serait pas exposée elle aussi.

Exigences

À compter du 14 octobre 2017,
tous les nouveaux marchands qui traitent des transactions de commerce électronique et des commandes par téléphone DOIVENT saisir la CVV2 et l'inclure dans la demande d'utilisation durant une transaction Visa. (Ne concerne pas les renseignements au dossier, les paiements récurrents ou par versement, les comptes commerciaux de carte virtuelle Visa et les transactions provenant de portefeuilles numériques).

- Si un émetteur approuve une transaction « sans correspondance » (c'est-à-dire une CVV2 est fournie, mais ne correspond pas au compte du titulaire de carte), alors l'émetteur est responsable du montant. Ainsi, les marchands bénéficient d'un niveau de protection supplémentaire.
- Aucun marchand au Canada ne sera autorisé à demander la CVV2 pour les transactions par la poste si les données sont fournies en format écrit. Cela réduit le risque de vol et d'usage frauduleux des renseignements en question.

Ces changements seront généralisés à TOUS les marchands qui traitent des transactions par commerce électronique ou par téléphone au Canada, et ce, d'ici le 13 octobre 2018.

3. Exploitation des données

Amélioration du processus d'autorisation

Situation actuelle

Avec l'évolution du système de paiement, les cas où la transaction est lancée en utilisant des renseignements enregistrés avec le consentement du titulaire de la carte pour une utilisation future ont augmenté considérablement.

La croissance du commerce numérique, ainsi que l'émergence de nouveaux modèles d'affaires, sont venues augmenter le nombre de transactions utilisant les renseignements de paiement du titulaire de la carte enregistrés pour de futurs achats.

La reconnaissance des transactions utilisant les renseignements d'identification enregistrés entraîne une meilleure évaluation du risque associé à une transaction, permettant ainsi un traitement robuste et différencié.

Exigences

À compter du mois d'octobre 2017 :
Les marchands et leurs agents tiers, facilitateurs de paiement ou opérateurs de portefeuilles numériques enregistrés qui offrent aux titulaires de carte la possibilité de consigner leurs renseignements au dossier doivent respecter ce qui suit :

- Communiquer aux détenteurs la façon dont les cartes seront utilisées.
- Obtenir le consentement des titulaires de carte à stocker les renseignements d'identification.
- Aviser les titulaires de carte lorsque des modifications sont apportées aux conditions d'utilisation.
- Aviser l'émetteur de la carte au moyen d'une transaction que les renseignements sur les paiements sont désormais consignés au dossier.
- Déterminer les transactions en utilisant des indicateurs adéquats lors de l'utilisation des renseignements enregistrés.

Que sont les renseignements enregistrés?

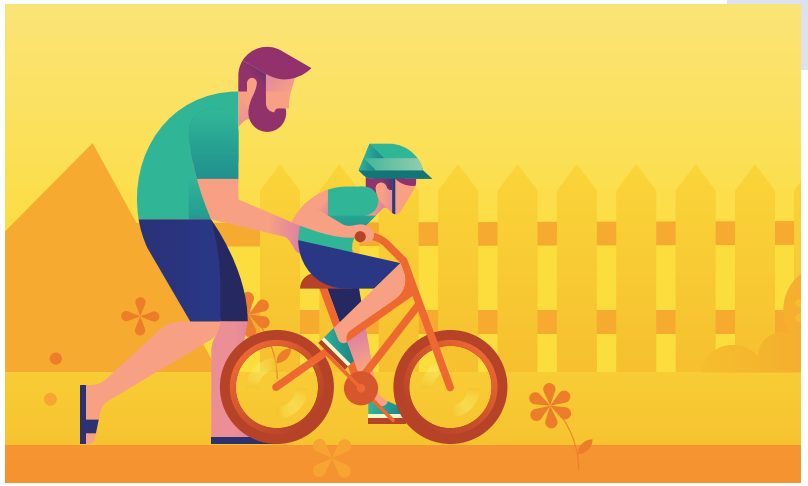
Les renseignements enregistrés sont de l'information (y compris, sans s'y limiter, un numéro de compte ou jeton de paiement) qui sont conservés par un marchand ou son agent, un fournisseur de traitement de paiement, ou un opérateur de portefeuille numérique pour traiter les transactions futures.

4. Habiliter toutes les personnes concernées

4. Habiliter toutes les personnes concernées

Bien que Visa et l'industrie des paiements comptent un certain nombre d'initiatives en place, la première ligne de défense contre la fraude par carte consiste à informer les marchands et les consommateurs, afin qu'ils puissent prendre des mesures de prévention de la fraude.

Visa a élaboré des outils de prévention de la fraude afin que les consommateurs, les banques et les marchands soient mieux outillés dans la lutte contre la fraude.



Pour les consommateurs :

Au Canada, tous les émetteurs peuvent fournir aux titulaires de carte de débit, de crédit et de cartes prépayées rechargeables Visa l'option de s'inscrire pour recevoir des alertes au sujet des transactions. Cela signifie que chaque fois que la carte d'un consommateur est utilisée, celui-ci reçoit un message de l'émetteur les avisant presque instantanément d'une transaction frauduleuse.

Exigences

À compter du 13 octobre 2018, tous les émetteurs de carte au Canada devront offrir aux titulaires de cartes de crédit, de débit et prépayées rechargeables Visa l'option de s'inscrire pour recevoir des alertes au sujet des transactions. Cette exigence s'applique à toutes les autorisations d'utilisation de la carte de marque Visa qui sont traitées par Visa, Interlink et Plus; elle ne s'applique pas aux cartes prépayées non rechargeables ou aux cartes commerciales.

Registre mondial des fournisseurs de services de Visa pour les banques et les marchands

La protection des données qui passent par le système du point de vente jusqu'à l'acquéreur est essentielle pour mériter la confiance de vos clients et la conserver. Le registre mondial des fournisseurs de services de Visa est à votre disposition pour vous aider à recourir à des agents compétents voués à sécuriser vos données. Les banques et les marchands devraient se rendre sur le site www.visa.com/splisting régulièrement dans leur quête de diligence raisonnable et utiliser uniquement des fournisseurs de services inscrits au registre pour externaliser leurs services de paiement par carte.

Conclusion

Conclusion

Feuille de route en matière de sécurité des paiements au Canada

2017

Utilisation élargie de la CVV2
- Les nouveaux marchands du commerce électronique et par téléphone doivent soumettre une CVV2 dans le cadre de leur autorisation
- Transfert de la responsabilité pour les approbations sans correspondance
- Les marchands de transactions par la poste ne doivent pas utiliser la CVV2 sur papier

2018

Utilisation élargie de la CVV2
- Tous les marchands du commerce électronique et par téléphone doivent soumettre une CVV2 dans le cadre de leur autorisation

Utilisation élargie du protocole 3DS
- Les émetteurs éliminent l'utilisation de mots de passe statiques pour 3DS
- Sensibilisation et information sur le protocole 3DS v2.0

Alertes pour les consommateurs
- L'émetteur doit fournir un service d'alertes aux consommateurs

Transaction de rechange par puce
- Les émetteurs doivent refuser une transaction de rechange par bande magnétique pour les transactions locales

2019

Utilisation élargie du protocole 3DS
- Activation du programme 3DS 2.0 à l'échelle mondiale

Données par bande magnétique sans contact
- Les marchands canadiens ne doivent pas accepter les transactions avec données par bande magnétique sans contact

2020 et après

Puce EMV
- Au Canada, tous les marchands doivent pouvoir traiter les transactions par puce EMV d'ici 2020 et les marchands munis de terminaux qui acceptent les demandes de titulaires de carte sans aide d'ici 2022

Conclusion

Visa collabore avec les intervenants de l'industrie, les décideurs, les autorités chargées de l'application de la loi et les consommateurs afin de garantir la sécurité des paiements et d'empêcher les fraudes. Nous adoptons une approche de sécurité multicouches qui a permis de maintenir le taux de fraude au minimum, malgré une croissance importante du volume des paiements par voie électronique.

Notre feuille de route canadienne est centrée sur quatre piliers :

1. Dévaluation des données en supprimant les données sensibles de l'écosystème et en rendant les renseignements sur comptes volés inutilisables (aucune transaction de rechange, terminaux pouvant accepter les cartes à puce (tous) et segmentation en unités).
2. Protection des données en instaurant des mesures de sécurité pour protéger les données à caractère personnel ainsi que les détails du compte (PCI DSS 3.2, éliminant le soutien des données par bande magnétique).
3. Exploitation des données en identifiant les fraudes possibles avant qu'elles ne se produisent et en augmentant le taux de confiance quant à l'approbation des transactions (3DS 2.0, CVV2)
4. Habilitation de toutes les personnes concernées y compris les consommateurs et les marchands pour lutter contre la fraude.

Visa est l'une des façons les plus sécuritaires et les plus sûres de payer et de recevoir des paiements. Comme pour toute nouvelle technologie, la sécurité continuera d'évoluer selon les besoins des consommateurs et la dynamique du marché. Bien que certains concepts exposés ici soient réels et déjà sur le marché, d'autres constituent des exemples possibles fondés sur les données dont on dispose à l'heure actuelle. À mesure que la technologie continuera de façonner notre industrie, Visa verra à mettre continuellement à jour cette feuille de route sur la sécurité afin d'atténuer les risques de fraude nouveaux et en constante évolution. Notre industrie est dynamique et Visa s'est engagée à rester à l'avant-garde du marché en s'adaptant aux besoins des consommateurs, des émetteurs, des acquéreurs et des marchands, et en continuant d'offrir des options de paiements numériques au quotidien de plus en plus sécuritaires pour tous, et en tout lieu.