Authentification forte du client :

Guide à l'attention des marchands

Septembre 2019

Avertissement

Cette présentation vous est fournie uniquement au titre de votre statut de client Visa et de participant au système de paiement Visa.
En acceptant cette présentation, vous reconnaissez que les informations qu'il contient (les « Informations ») sont confidentielles et soumises aux restrictions de confidentialité contenues dans les Règles de Visa ou d'autres accords de confidentialité qui limitent votre utilisation des Informations.

Vous acceptez de garder ces Informations confidentielles et de ne pas les utiliser à des fins autres que celles qui vous incombent en tant que client de Visa ou en tant que participant au système de paiement Visa. Les informations ne peuvent être diffusées au sein de votre entreprise que sur la base de la nécessité de savoir pour vous permettre de participer au système de paiement Visa. Veuillez noter que les Informations peuvent constituer des informations non publiques importantes au sens des lois sur les valeurs fédérales américaines et que l'achat ou la vente de valeurs de Visa Inc., tout en étant au courant d'informations non publiques importantes, constituerait une violation des lois sur les valeurs fédérales américaines applicables.

Des études de cas, des comparaisons, des statistiques, des recherches et des recommandations sont fournies « en l'état » et à des fins d'information uniquement. Elles ne doivent pas être utilisées en tant que conseils opérationnels, marketing, juridiques, techniques, fiscaux, financiers ou autres.

Les produits et services décrits dans ce document peuvent faire l'objet de développements ultérieurs et les dates de lancement de caractéristiques spécifiques ne sont données qu'à titre indicatif. Visa se réserve le droit de réviser ce document en conséquence.

En tant que nouveau cadre réglementaire dans un écosystème en constante évolution, les exigences en matière de SCA doivent encore être affinées pour certains cas d'utilisation.
Ce document reflète l'évolution de la pensée de Visa, mais il ne doit pas être considéré comme une position définitive ni comme un avis juridique. Il peut être modifié en fonction des indications et des éclaircissements fournis par les autorités compétentes. Visa se réserve le droit de réviser ce document au regard des futurs développements réglementaires. Nous encourageons les clients à contacter Visa s'ils rencontrent des difficultés en raison de directives contradictoires émanant des autorités de réglementation locales. Lorsque cela se justifie, Visa collaborera de manière proactive avec les organismes de réglementation pour tenter de résoudre ces problèmes.

Ce guide ne vise pas non plus à garantir ou à assurer le respect des exigences réglementaires. Les prestataires de services de paiement sont responsables de leur propre conformité aux exigences de la SCA et sont encouragés à demander conseil à un professionnel compétent, le cas échéant.

Bonjour

Nous avons créé ce guide pour aider votre entreprise à se préparer à l'introduction dans toute l'Europe de l'authentification forte du client (Strong Customer Authentication ou « SCA »).

La SCA sera utile à tous ceux qui effectuent et acceptent des paiements Visa. Elle réduira les risques de fraude et améliorera la sécurité. C'est une bonne nouvelle pour les entreprises (comme la vôtre) et pour les consommateurs.

Ce guide contient des conseils qui aideront votre entreprise et votre personnel à se préparer aux changements à venir. Il explique aussi pourquoi il est important de contacter votre prestataire de service de paiement (Payment Service Provider, PSP).
Enfin, il contient des éléments de communication qui vous aideront à sensibiliser les clients à propos des changements sur votre site web et en magasin.

Ce contenu n'a pas de référence légale et n'est en aucun cas un conseil professionnel. Les prestataires de services de paiement sont responsables de leur propre conformité aux exigences PSD2 et de leurs propres communications avec les clients. Ce contenu doit être lu avec la diapositive 2.
Ce guide a été publié en septembre 2019.

Table des matières

1. Comprendre la SCA

1.1 La SCA en quelques mots

L’Union européenne introduit de nouvelles mesures de sécurité appelées Authentification forte du client (Strong Customer Authentication ou SCA) qui pourraient changer la manière dont les clients paient en ligne et hors ligne/en magasin en effectuant un paiement sans contact avec leur carte Visa.

Toutes les entreprises basées dans l’Espace économique européen (EEE) ou desservant des clients qui s’y trouvent et qui acceptent des paiements par carte de crédit ou de débit seront concernées.

Ces lois introduisent des mesures de sécurité appelés authentification à deux facteurs pour renforcer la sécurité des clients lorsqu’ils effectuent des transactions de paiement, y compris en ligne et sans contact. Ce changement concerne toute l’industrie.

Dans le cadre des changements, les banques recevront plus de données pour prendre des décisions informées à propos de la nécessité ou non de l’authentification à deux facteurs.
Les solutions SCA de Visa emploient la technologie la plus récente, qui analyse le risque plus rapidement pour créer une expérience de paiement encore plus fluide.

Les niveaux accrus de sécurité et de contrôle bénéficieront directement aux clients en renforçant leur confiance lors de leurs achats en ligne ou en magasin.

Visa collabore étroitement avec les émetteurs participants et votre PSP pour contribuer à protéger les clients de l'utilisation non autorisée de leur carte quand ils font des achats en ligne ou hors ligne.

1.2 Authentification à deux facteurs

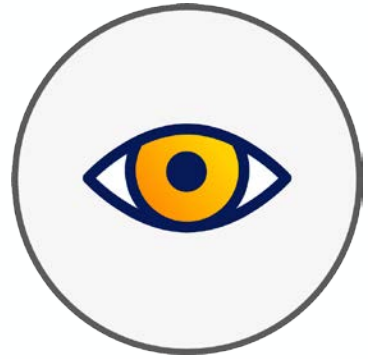
Après la mise en œuvre de la SCA, vos clients devront peut-être confirmer leur identité en passant par une étape de sécurité supplémentaire quand ils paient avec leur carte de paiement Visa. On parle d' **authentification à deux facteurs**, ce qui signifie qu'ils devront peut-être fournir des informations provenant d'au moins deux des trois catégories suivantes. Les informations qu'ils doivent fournir dépendront des exigences de leur banque.

Un élément que vous connaissez

comme un mot de passe ou un code PIN

Un élément que vous possédez

comme un téléphone mobile, lecteur de carte, ou autre appareil



Un élément que vous êtes

comme un lecteur d'iris, la reconnaissance faciale ou une empreinte digitale

Votre PSP peut vous indiquer ce que vous devez faire pour vous préparer et vous expliquera le calendrier de mise en œuvre. Ces éléments sont actuellement à l'étude par certains régulateurs locaux européens. Votre PSP peut également avoir des informations sur les changements sur son site web.

1.3 L’impact potentiel de la SCA sur votre entreprise

La SCA est une opportunité pour vous et vos clients car elle rend les paiements encore plus sûrs et offre encore plus de protection contre le risque de fraude.

Si votre entreprise est préparée à la SCA, vous pourrez offrir à vos clients une expérience de paiement Visa rapide et facile, et vous bénéficierez des améliorations à venir.

Ce que la SCA pourrait signifier pour votre activité :

L’authentification des clients arrive – Selon le groupe de pilotage des émetteurs britanniques Visa, les émetteurs prévoient de demander l’authentification des clients pour un plus grand nombre de transactions.[1]

Soyez prêts pour la SCA – Une récente étude a révélé que seulement 15 % des entreprises se sentaient « extrêmement bien préparées » à la SCA et seulement 40 % prévoient d’être prêtes d'ici septembre 2019.[2]

L’expérience de vos clients doit rester fluide pour les fidéliser –
52 % des clients qui abandonnent leur panier font leurs achats chez un autre marchand qui offre un meilleur flux de paiement.[3]

Contactez votre PSP pour discuter des améliorations qui doivent être apportées afin d’introduire le nouveau processus d’authentification dans votre parcours de paiement Visa. Vous garantirez ainsi la pérennité de la réussite de votre activité tout en vous démarquant de vos concurrents.

[1] Visa UK Authentication Steering Group ; février 19.
[2] The impact of SCA, 451 Research ; mai 19.
[3] The impact of SCA, 451 Research ; mai 19.

1.4 Tout ce que vous devez prendre à compte à propos de la SCA

Faites évoluer votre activité – Pour continuer à accepter les paiements Visa en ligne et sans contact rapidement et facilement après l'introduction de la SCA.
Vous pouvez parler des éventuelles améliorations avec votre PSP, participer à 3DS, profiter au maximum des exemptions ou mettre à niveau votre terminal au point de vente. Vous pourrez ainsi optimiser l'expérience de paiement de vos clients et profiter au maximum des opportunités offertes par la SCA.

L'engagement de Visa à améliorer la sensibilisation à la SCA – Pour vous aider à présenter les améliorations qui seront introduites par la SCA et leurs avantages, nous avons joint à ce guide une série de communications.

Une expérience client totalement fluide – Si vous comprenez bien le fonctionnement de la SCA, vous garantirez à vos clients un parcours de paiement fluide et ils continueront à faire leurs achats chez vous.

Pour que votre entreprise soit prête à la SCA, contactez votre PSP dès aujourd'hui.

2. L’expérience de la SCA pour le client

2.1 Ce que signifiera la SCA pour vos clients

Quand la SCA sera entera en vigueur, votre entreprise et vos clients bénéficieront d’une sécurité renforcée et d'un risque de fraude réduit.

La SCA a pour but d'aider les marchands en renforçant la sécurité des transactions, en améliorant l’expérience clients et en augmentant le nombre de ventes conclues.

Pour les clients, son but est de rassurer, grâce à une meilleure protection contre la fraude et à des passages en caisse fluides.

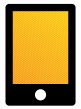
2.2 Expérience du client en ligne

En ligne

Voici comment vos clients effectueront des paiements Visa quand la SCA sera requise.

Les clients devront parfois confirmer leur identité quand ils effectueront un paiement en utilisant la méthode d'authentification choisie par leur banque. Pour cela, ils devront fournir des informations provenant d'au moins deux des trois catégories ci-dessous (authentification à deux facteurs).

Un élément qu'ils connaissent – comme un mot de passe ou un code PIN



Un élément qu'ils possèdent - comme un téléphone mobile, un lecteur de carte ou autre appareil

Un élément qu'ils sont - comme un lecteur d'iris, la reconnaissance faciale ou une empreinte digitale

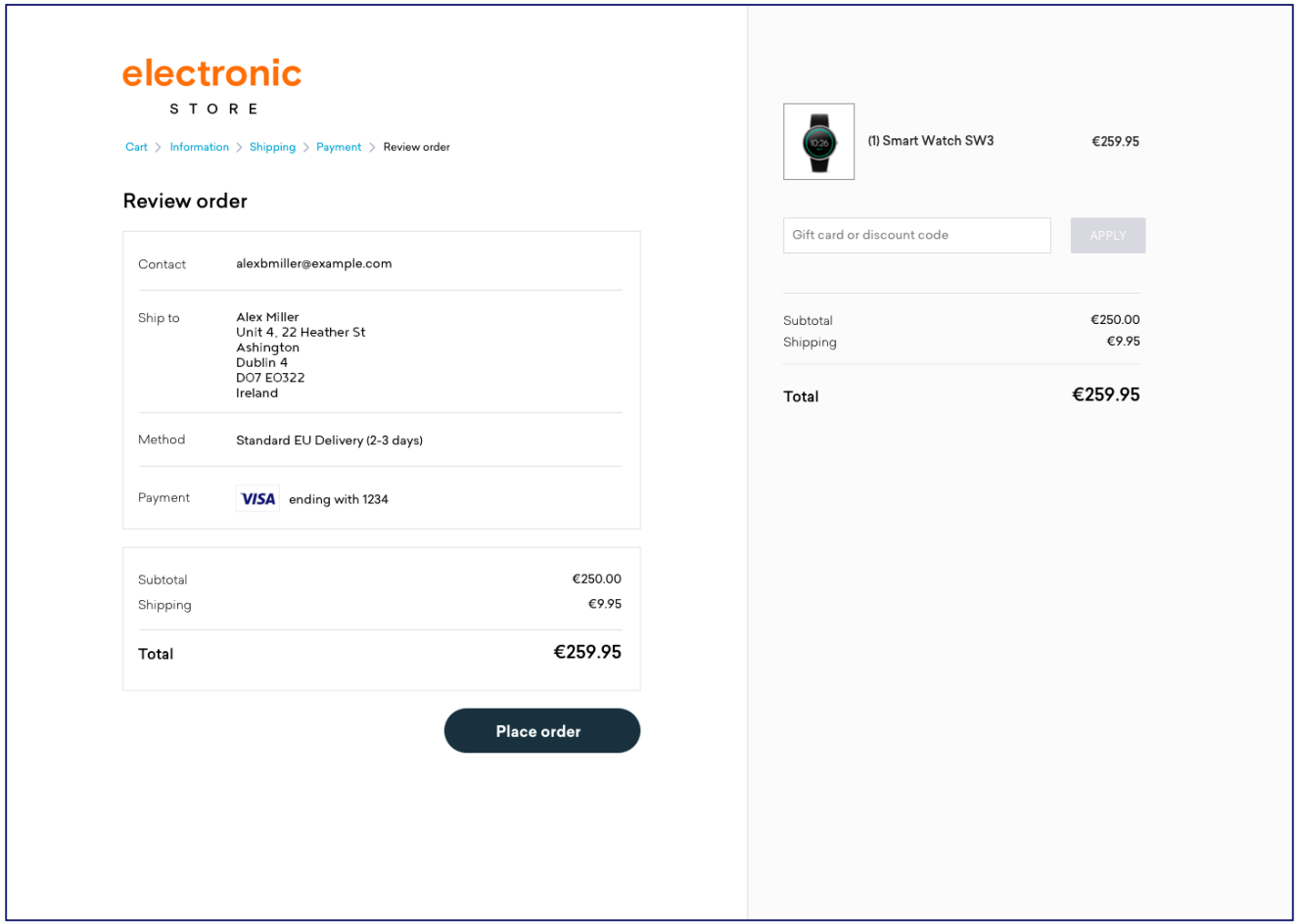
2.2 Expérience du client en ligne

Voici comment vos clients effectueront des paiements Visa quand la SCA aura été mise en œuvre :

Étape 1.

Un client souhaite effectuer un achat en ligne sur son ordinateur de bureau ou portable, son téléphone portable ou depuis un autre appareil numérique et accède à la page de paiement du vendeur.

Conseil :
Si un client vous contacte à propos de problèmes liés à l'authentification, renvoyez-le à sa banque émettrice qui lui fournira plus d'informations.



Le magasin électronique est un exemple que le marchand a créé pour démontrer uniquement le processus d'achat.

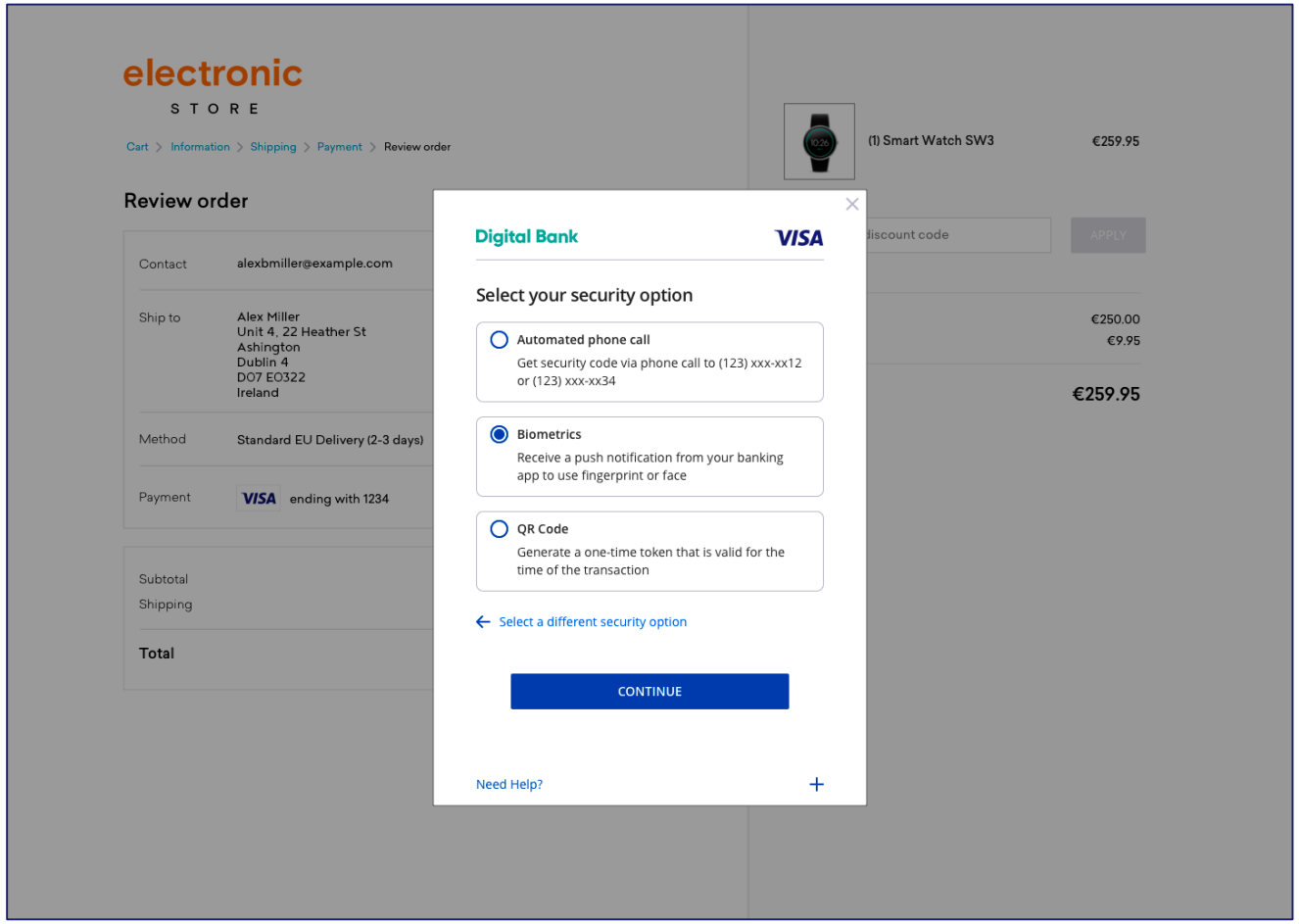
Ce contenu n'a pas de référence légale et n'est en aucun cas un conseil professionnel. Les prestataires de services de paiement sont responsables de leur propre conformité aux exigences PSD2 et de leurs propres communications avec les clients. Ce contenu doit être lu avec la diapositive 2. Ce guide a été publié en septembre 2019.

2.2 Expérience du client en ligne

Voici comment vos clients effectueront des paiements en ligne quand la SCA aura été mise en œuvre :

Étape 2.

Pour terminer la transaction, ils peuvent choisir leur méthode de vérification ou utiliser celle choisie par leur émetteur.



Conseil :
Si un client vous contacte à propos de problèmes liés à l'authentification, renvoyez-le à sa banque émettrice qui lui fournira plus d'informations.

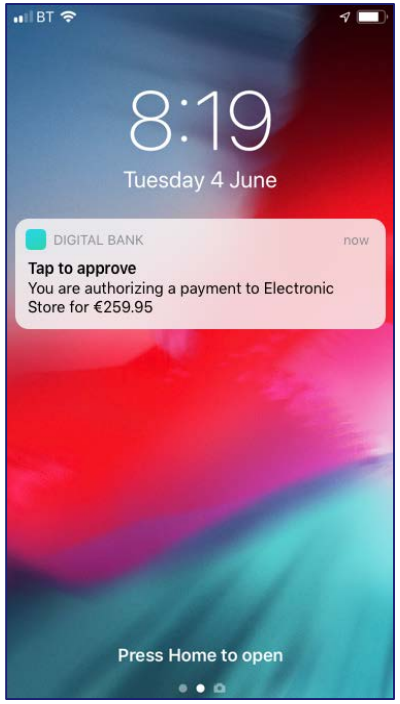
Le magasin électronique est un exemple que le marchand a créé pour démontrer uniquement le processus d'achat.

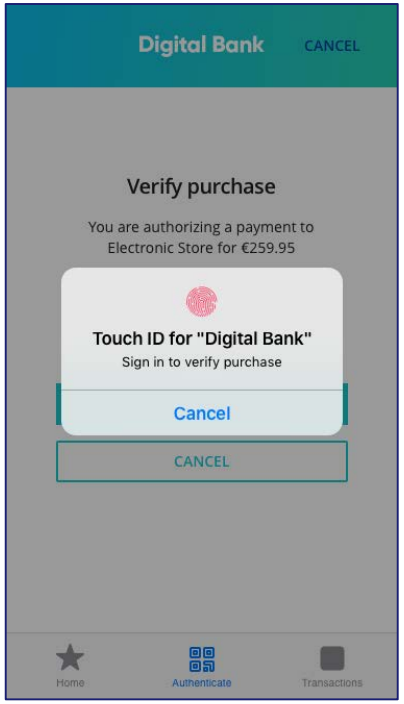
2.2 Expérience du client en ligne

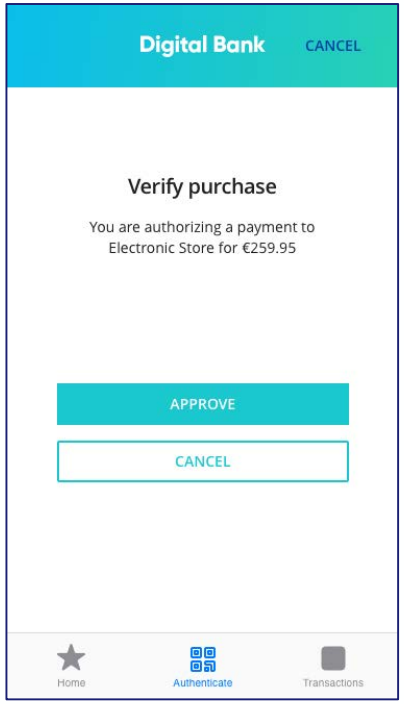
Voici comment vos clients effectueront des paiements en ligne quand la SCA aura été mise en œuvre :

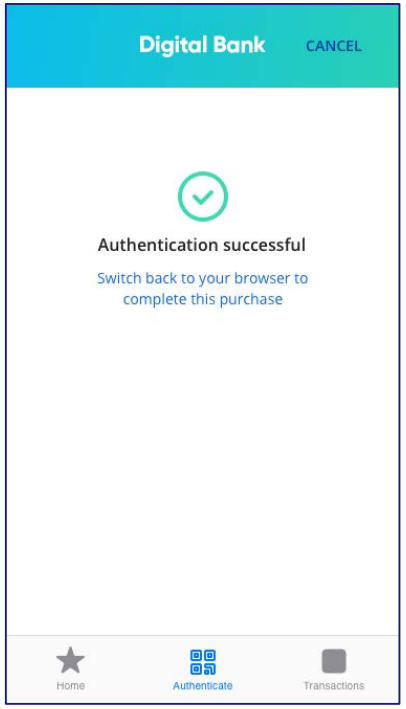
Étape 3.

Il leur suffit de suivre les instructions pour terminer leur achat.









Conseil :
Si un client vous contacte à propos de problèmes liés à l'authentification, renvoyez-le à sa banque émettrice qui lui fournira plus d'informations.

Le magasin électronique est un exemple que le marchand a créé pour démontrer uniquement le processus d'achat.

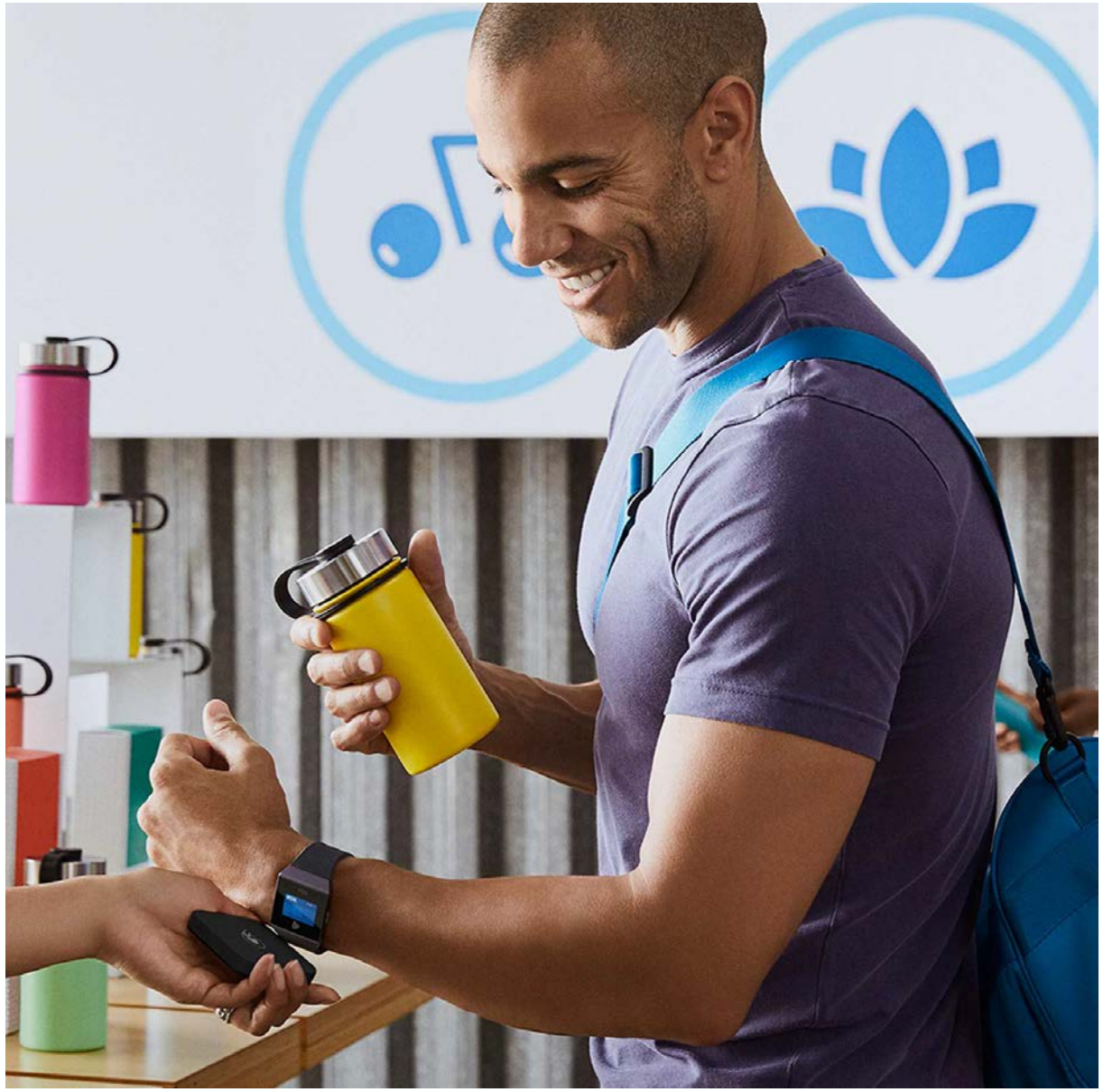
2.3 Expérience du client en magasin

Les clients devront parfois saisir leur code PIN plus souvent s'ils paient en sans contact :

- S’ils effectuent plus de (5)** achats sans contact consécutifs sans fournir d’authentification, ou ;
- Si la valeur cumulée des paiements sans contact depuis la dernière demande d'authentification supplémentaire dépasse (150 €)** au total, ou ;
- Si une banque émettrice souhaite vérifier l’identité du client.

Conseil :
Si le client ne peut pas conclure la transaction sans contact après avoir saisi son code PIN, demandez-lui d'insérer sa carte et de saisir son code PIN pour effecteur un paiement puce + PIN.

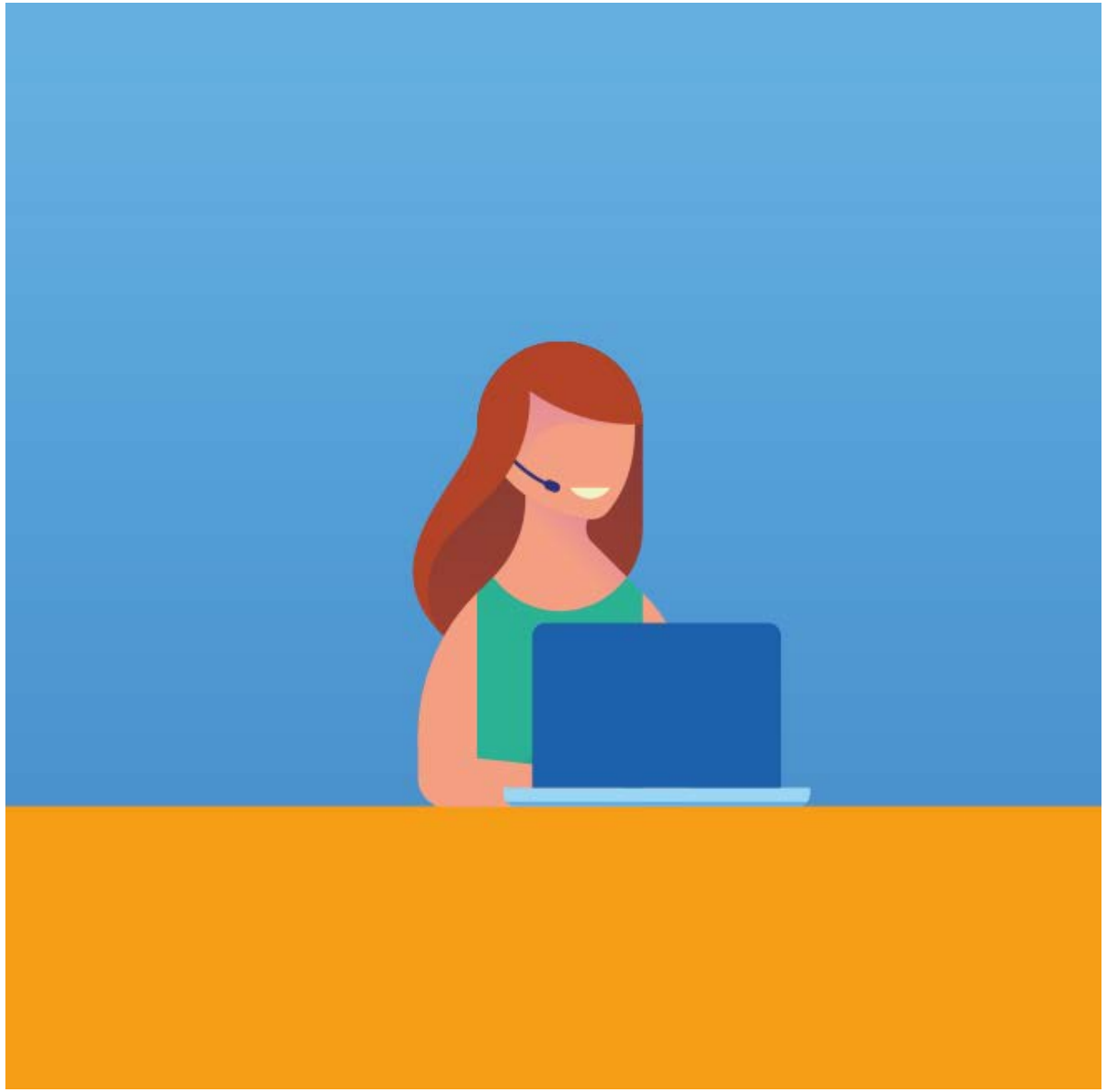
Si le problème persiste, demandez-lui de contacter sa banque émettrice qui pourra lui donner des informations complémentaires.



** Dépend de l'implémentation de l'émetteur.

3. Appliquer la SCA

3.1 Parler à votre PSP



Les marchands tels que vous ont un rôle à jouer pour réduire la fraude et améliorer l'expérience du client.

Votre entreprise doit donc se préparer à la SCA pour éviter dans la mesure du possible que les banques émettrices refusent des transactions.

Demandez à votre PSP :

- ce que vous devez faire
- ce que cela pourra signifier pour votre activité
- comment soutenir une expérience de paiement fluide pour les clients.

Les sections suivantes présentent les aspects que vous devrez sans doute aborder avec lui, que votre activité soit en ligne, en magasin ou les deux, ou encore si vous souhaitez bénéficier des exemptions de la SCA.

3.2 Mise en œuvre pour le commerce en ligne

Vous devez parler à votre PSP pour vous aider à intégrer les modifications au plan technologique afin de traiter les paiements en ligne.

Contactez votre PSP :
Quand vous aurez mis en œuvre le 3DS par le biais de votre PSP, il vous fournira le badge « Visa Secure » (signalétique) pour votre commerce en ligne.

Pour promouvoir une excellente expérience de paiement en ligne pour vos clients :

- Inscrivez-vous pour pouvoir utiliser l'authentification **3-D Secure (3DS)** – Visa offre ce service via Visa Secure. Sans Visa Secure, il est possible que vos clients ne puissent pas conclure leurs transactions en ligne.
- Passez à la nouvelle version de 3DS – la version la plus récente est 3DS 2.2 – pour une meilleure expérience client, surtout quand les achats sont faits sur une tablette et sur smartphone. Cette version offre également des avantages importants pour votre activité.

3.3 Mise en œuvre pour les magasins traditionnels

Les paiements puce + PIN en magasin ne changeront pas. Pour les paiements sans contact, les titulaires de cartes peuvent se voir demander de saisir leur code PIN plus souvent.

Codes de réponse
À l'heure actuelle, quand votre PSP traite une transaction, il vous envoie un code de réponse à deux chiffres émis par la banque émettrice pour vous informer du statut du paiement. Le statut vous indique si le paiement a été approuvé ou refusé, voire des mesures à prendre. Ces codes de réponse vont être complétés pour l'introduction de la SCA.

Comment les codes de réponse vont-ils changer ?
Pendant le processus de transaction, deux nouveaux codes de réponse seront activés dans les cas suivants :
Le montant du paiement est supérieur à 50€ et

- les clients ont effectué plus de (5)** achats sans contact consécutifs depuis leur dernière authentification forte

ou
Le montant du paiement est supérieur à 50€ et

- la valeur cumulée des paiements sans contact depuis la dernière authentification forte dépasse 150 €**

ou

- L'émetteur souhaite vérifier l'identité du client.

Ce sont les PSPs qui contrôlent les nouveaux codes de réponse. Si les émetteurs dans n'importe quel pays de l'EEE utilisent les nouveaux codes de réponse, les PSPs et les marchands doivent être prêts et vérifier que leurs terminaux peuvent prendre en charge les nouveaux codes :

1. **Code de réponse 70** – s'applique aux transactions PIN en ligne et demande au client de saisir son code PIN.
2. **Code de réponse 1A** – s'applique aux transactions PIN hors ligne et demande au terminal de changer d'interface pour l'insertion de la carte dans le terminal et la saisie d'un code PIN.

Contactez votre PSP
Il pourra vous aider à intégrer les modifications dans votre système.

** Dépend de l'implémentation de l'émetteur.

3.4 Profiter des exemptions

Contactez votre PSP
Comprenez comment votre entreprise peut profiter des exemptions à la SCA et des transactions non concernées pour offrir à vos clients une expérience de paiement fluide.

Voici des exemples de situations dans lesquelles les clients n'auront pas besoin d'utiliser l'authentification à deux facteurs pour effectuer des paiements.

- **Pour les paiements sans contact de moins de 50€ *** (Mais, après cinq transactions consécutives, ou si la valeur cumulée des paiements sans contact depuis la dernière fois où une authentification supplémentaire a été fournie dépasse 150 €*, le client devra peut-être saisir son code PIN.)

- **Paiements en ligne à faible risque.** Dans le cadre des nouvelles mesures de sécurité, les banques pourront prendre plus rapidement de meilleures décisions d'analyse des risques car elles recevront des données plus fines. La SCA n'est pas nécessaire si un paiement en ligne est déterminé par l'analyse des transactions en temps réel comme présentant peu de risques.

- **Marchands de confiance.** Les titulaires de carte peuvent ajouter à une liste les magasins auxquels ils font confiance pour éviter d'avoir à fournir la SCA quand ils font des achats chez ce marchand.**

- **Paiements d'entreprise.** Certains paiements d'entreprise effectués selon des processus dédiés peuvent être exemptés si le régulateur local considère qu'ils sont suffisamment sécurisés (par exemple les cartes dites « logées » ou virtuelles).

*Dépend de la limite de la somme autorisée pour un paiement sans contact dans le pays concerné. (CVM - Méthode de vérification du client).
**Bientôt disponible sur votre marché. Demandez des précisions à votre PSP.

3.4 Profiter des exemptions

Contactez votre PSP
Comprenez comment votre entreprise peut profiter des exemptions à la SCA et des transactions non concernées pour offrir à vos clients une expérience de paiement fluide.

Voici des exemples de situations pour lesquelles les clients n'auront pas besoin d'utiliser l'authentification à deux facteurs pour effectuer des paiements.

- **Paiements à faible valeur en ligne.** Tout comme les paiements sans contact, les paiements inférieurs à 30 € sont exemptés de la SCA mais si l'exemption a été utilisée cinq fois depuis la dernière authentification forte du client ou si les paiements dépassent 100 €, la banque peut demander une authentification.

- **Automates de transport ou de stationnement.** Le paiement de titres de transport ou de stationnement sur des terminaux automatisés (par ex. dans un aéroport ou une gare) n'exigeront pas la SCA**.

**Si un émetteur applique une « solution basée sur la carte », la SCA peut être déclenchée dans certains cas uniques, pour lesquels le titulaire de carte ne pourra pas remplir les exigences de la SCA telles que la saisie de son code PIN.

3.5 Transactions auxquelles la SCA ne s'applique pas (hors du périmètre)

Il existe des transactions auxquelles la SCA ne s'applique pas. La liste de droite n’est pas exhaustive. Veuillez consulter la page 2.

- **Transactions initiées par les marchands (MIT).** Il s’agit notamment des abonnements et les versements convenus à l’avance avec le titulaire de carte et initiés par le marchand. Au moment de la mise en place d'un nouvel abonnement ou de l’adhésion, on demandera aux clients de s’authentifier.

- **Paiements par correspondance ou par téléphone (MOTO).** Aucun paiement effectué par téléphone ou par correspondance n’exigera une authentification.

- **Une transaction pour laquelle l’émetteur ou le PSP sont situés en dehors de l'EEE.**
  En tant que marchand situé dans l’EEE, votre PSP devra cependant faire de son mieux pour appliquer la SCA dans la mesure du possible.

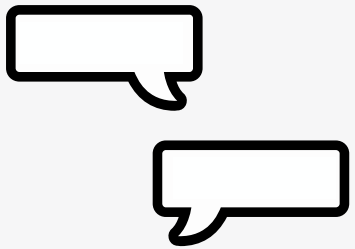
- **Transactions anonymes.** Les transactions effectuées au moyen d’instruments de paiement anonymes tels une carte prépayée anonyme ne sont pas soumises aux exigences de SCA.

4. Comment communiquer avec les clients

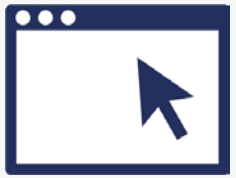
4.1 Comment expliquer la SCA à vos clients

Pour assurer la réussite de la SCA, votre personnel et vos clients doivent impérativement connaître les améliorations qu'elle introduira.

Pour vous aider à communiquer ces améliorations à votre personnel, nous avons créé plusieurs documents :



Aide aux conversations



Messages sur le site web

Manuel destiné au personnel avec FAQ

Ces documents devraient rassurer vos collaborateurs et leur donner confiance à propos des développements à venir liés à la SCA.

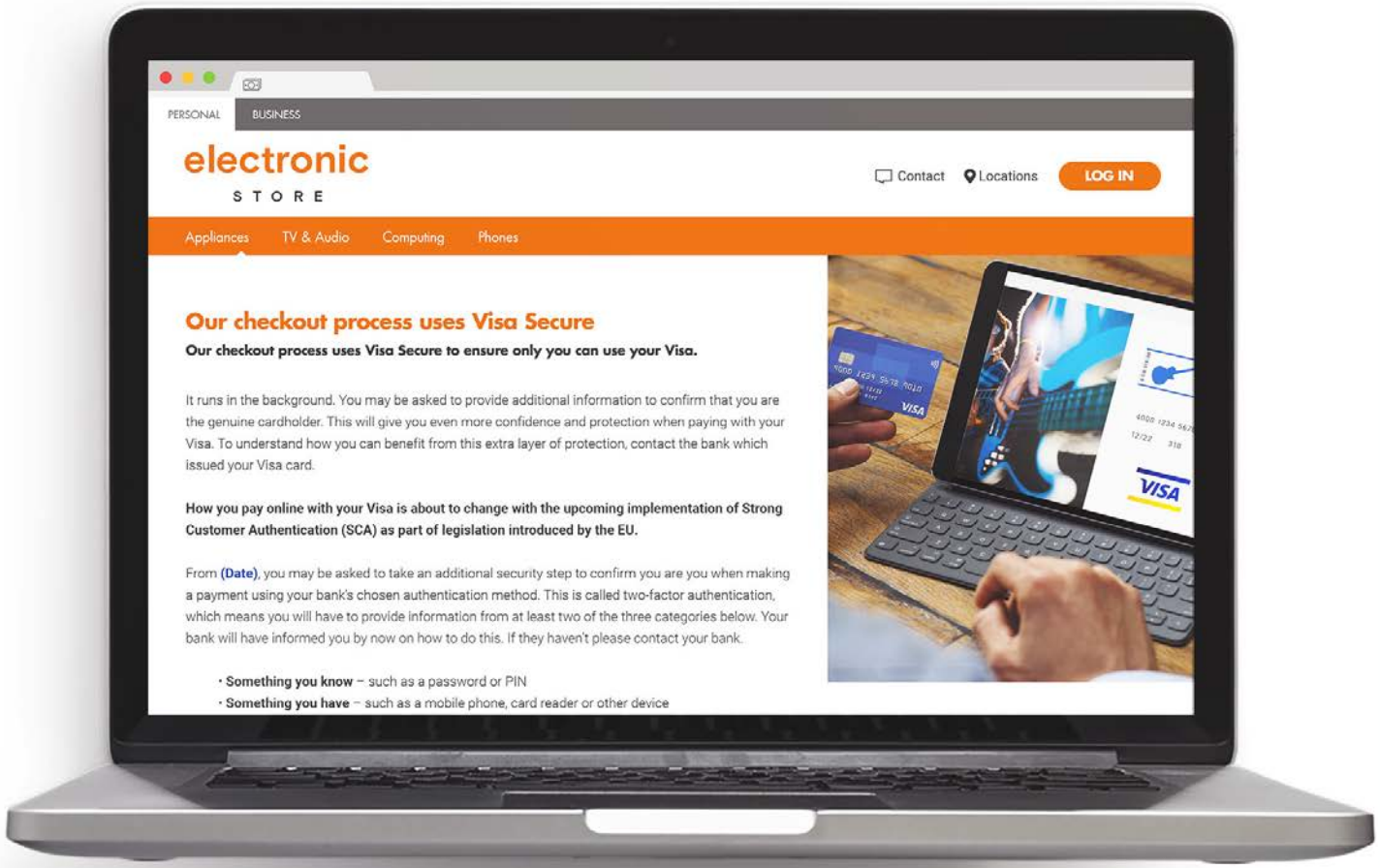
La banque émettrice du client est la mieux placée pour fournir des informations détaillées sur la SCA, telles que les mesures anti-fraude et la sécurité des paiements. Si votre client a des questions spécifiques à propos de la SCA, assurez-vous que vos collaborateurs savent qu'ils doivent diriger le client vers son émetteur.

4.2 Conseils de communication pour le commerce en ligne

4.2.1 Paragraphe sur le site web

Voici un exemple de communication que nous recommanderions pour présenter la SCA sur votre site web, sur la page que vous estimez appropriée (par exemple la page FAQ, la page d'aide ou la page paiement).

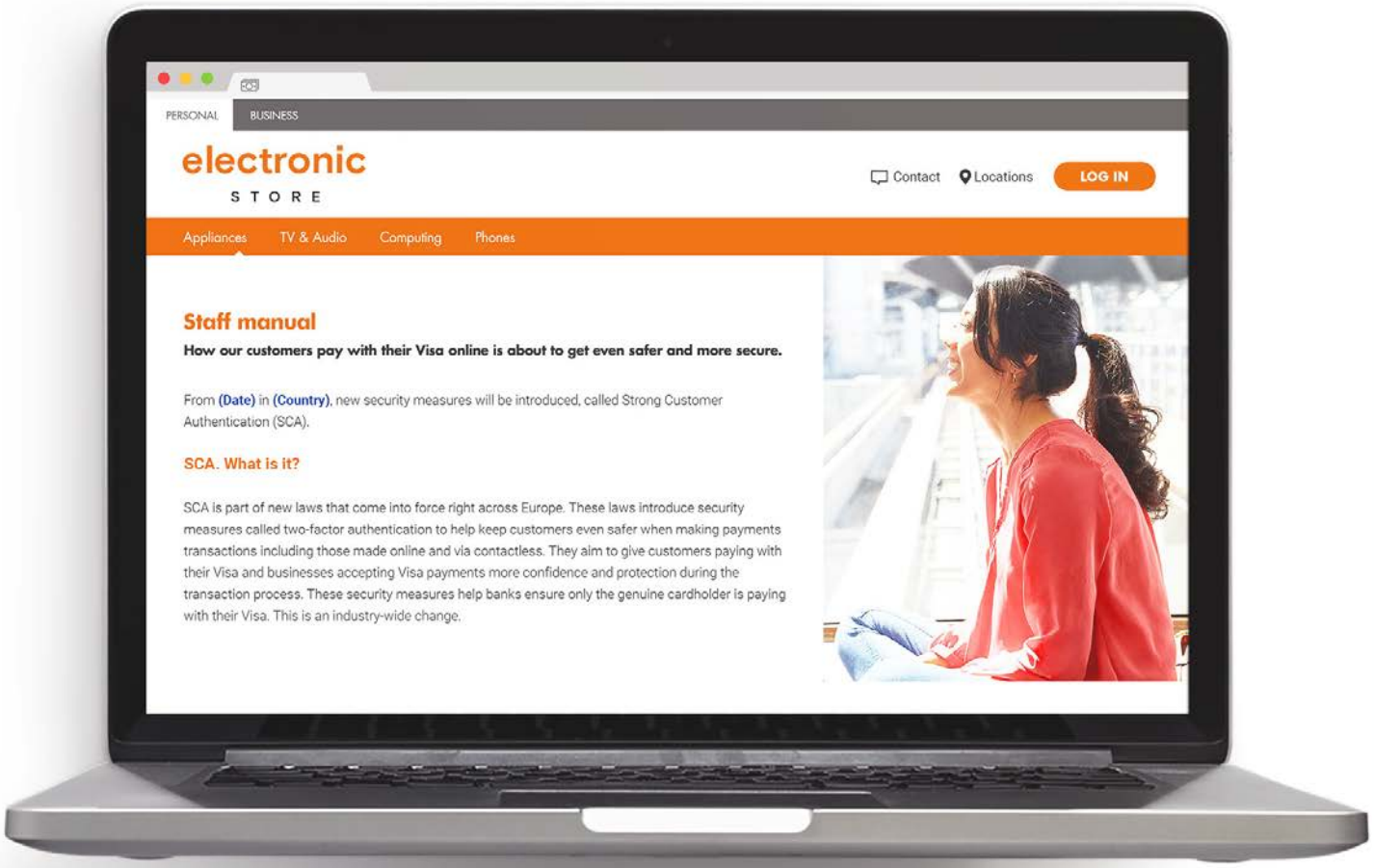
Voir le texte complet page 34 ❯



4.2 Manuel du personnel

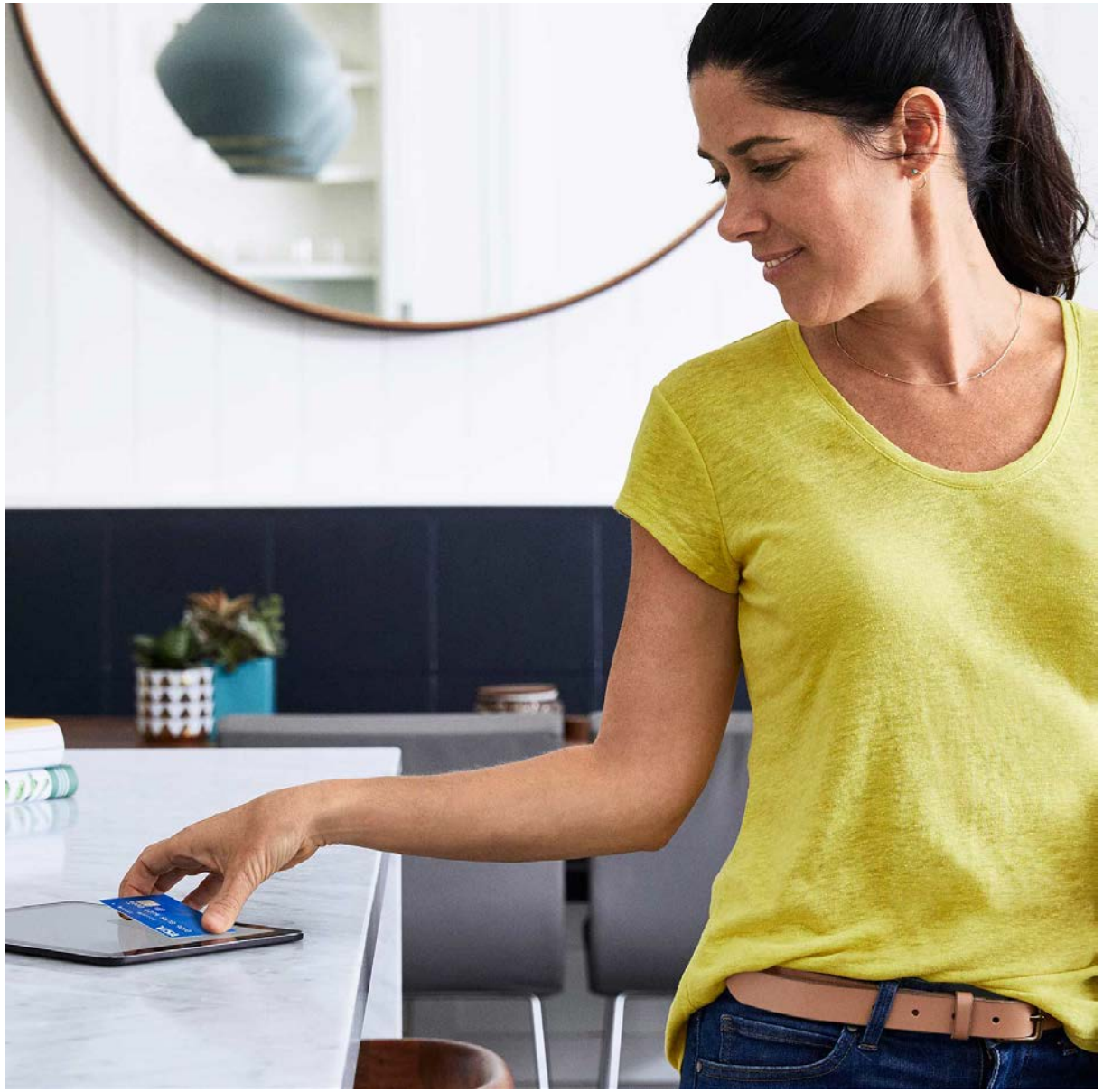
Voici un exemple de manuel à l'attention de vos employés pour expliquer la SCA. Cette communication contient les informations de contexte nécessaires pour pouvoir répondre à des questions courantes des clients, ce qui contribuera à éviter toute perturbation de votre activité.

Voir le texte complet page 35 ❯



4.2.3 Indication sur le site web

Vous pouvez utiliser le badge Visa Secure sur votre site web.
Quand vos clients voient « Visa Secure », ils peuvent être sûrs que leur transaction est protégée par plusieurs niveaux de sécurité. Contactez votre PSP pour obtenir le badge.

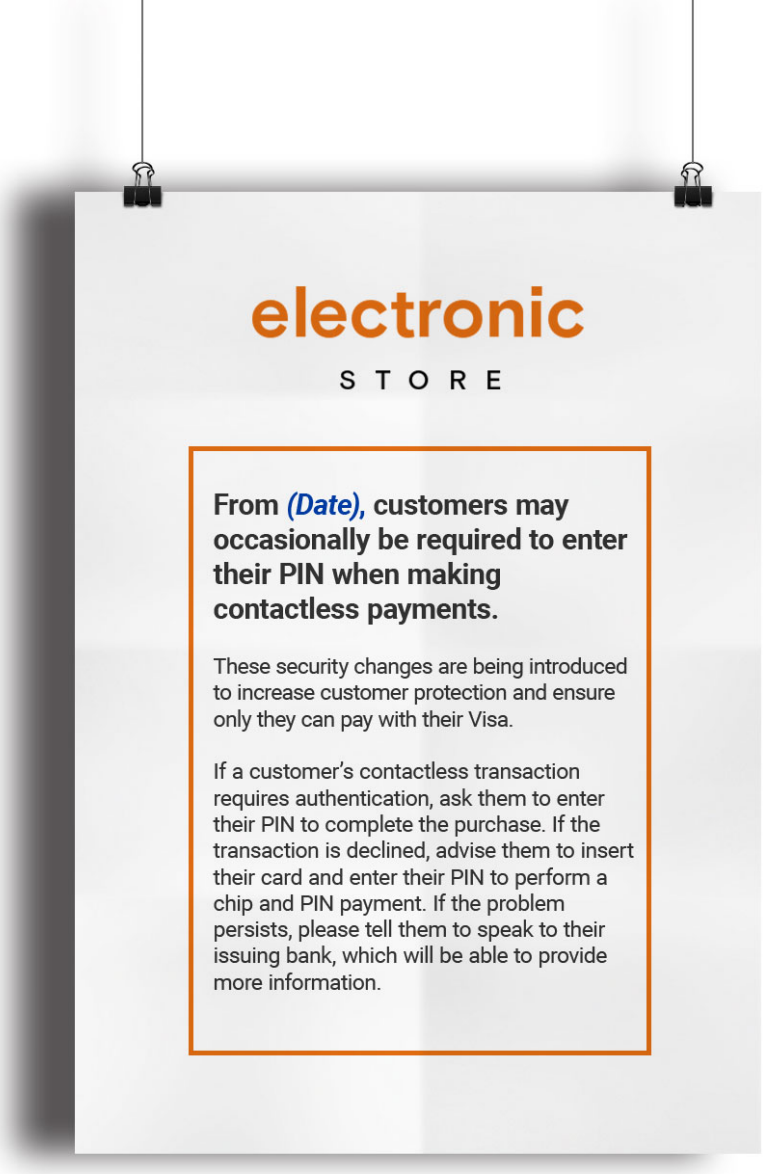


4.3 Conseils de communication pour les magasins traditionnels

4.3.1 Aide aux conversations

Voici un exemple d'une version plus concise du manuel destiné au personnel. Ce document peut être placé à côté des caisses en magasin pour aider les nouveaux employés qui n'ont pas encore suivi une formation.

Voir le texte complet page 39 ❯



4.3 Manuel du personnel

Voici un exemple de communication pour votre personnel. Il donne les informations de contexte et montre comment répondre à certaines questions courantes des clients.

Voir le texte complet page 40 ❯

Annexe : Matériel de communication détaillée

Vous trouverez ici quelques messages recommandés à destination des titulaires de carte.
Il s'agit de documents pour vous guider, que vous pouvez utiliser dans votre communication.

Annexe 4.2.1

Paragraphe sur le site web

Voici un exemple de la communication que nous recommanderions pour présenter la SCA sur votre site web commercial, sur la page que estimez appropriée (par exemple la page FAQ, la page d'aide ou pendant le processus de paiement).

Notre processus de paiement utilise Visa Secure
Notre processus de paiement utilise Visa Secure pour garantir que vous seul puissiez utiliser votre carte Visa. Il se déroule en arrière-plan.
On pourrait vous demander de fournir des informations supplémentaires pour confirmer que vous êtes bien le titulaire de la carte. Cela vous donnera encore plus de confiance et de protection lorsque vous payez avec votre carte Visa. Pour connaître les avantages de ce niveau supplémentaire de protection, contactez la banque qui a émis votre carte Visa.

Votre manière de payer en ligne avec votre carte Visa est sur le point de changer avec la mise en œuvre prochaine de l'authentification forte du client (SCA) dans le cadre d'une législation introduite par l'Europe.

À partir du 14 septembre 2019, on pourra vous demander de franchir une étape de sécurité supplémentaire pour confirmer votre identité lorsque vous effectuez un paiement avec la méthode d'authentification choisie par votre banque. Ceci s'appelle « authentification à deux facteurs », ce qui signifie que vous devrez fournir des informations provenant d'au moins deux des trois catégories suivantes. Votre banque vous aura expliqué comment vous y prendre. Si ce n'est pas le cas, contactez la.

- **Un élément que vous connaissez** – comme un mot de passe ou un code PIN
- **Un élément que vous possédez** - comme un téléphone mobile, un lecteur de carte ou autre appareil
- **Un élément que vous êtes** - comme un lecteur d'iris, la reconnaissance faciale ou une empreinte digitale

Utilisez cette section si votre entreprise offre des abonnements ou des paiements récurrents.
Vous devrez confirmer votre identité quand vous mettrez en place un nouvel abonnement ou un paiement récurrent. Les paiements subséquents et les abonnements existants n'exigeront pas l'authentification à deux facteurs, mais une authentification pourra être nécessaire si vous apportez des modifications à votre abonnement.

Annexe 4.2.2

Manuel du personnel

Voici un exemple d'un manuel du personnel qui présente la communication à votre personnel que nous recommanderions à propos de la SCA. Cette communication contient les informations de contexte nécessaires pour que vos collaborateurs puissent répondre à des questions courantes des clients, ce qui contribuera à éviter toute perturbation de votre activité.

Les paiements en ligne de nos clients avec leur carte Visa seront bientôt encore plus sûrs et sécurisés.

De nouvelles mesures de sécurité seront introduites, appelées Authentification forte du client (Strong Customer Authentication, SCA).

Sur la SCA. De quoi s'agit-il ?
La SCA fait partie des nouvelles lois qui entrent en vigueur partout en Europe. Ces lois introduisent des mesures de sécurité appelés authentification à deux facteurs pour renforcer la sécurité des clients lorsqu'ils effectuent des transactions de paiement, y compris en ligne et sans contact. Leur but est de donner aux clients qui utilisent leur carte Visa pour payer, et aux entreprises qui acceptent les paiements Visa plus de confiance et de protection pendant le processus de transaction. Ces mesures de sécurité aideront les banques à s'assurer que c'est exclusivement le titulaire de carte qui paie avec sa carte Visa. Ce changement concerne toute l'industrie.

Comment les choses se passeront-elles quand un client fera ses achats chez nous ?
Quand un client paie avec sa carte Visa, on pourra lui demander de franchir une étape de sécurité supplémentaire pour confirmer son identité en utilisant la méthode d'authentification choisie par sa banque. Ceci s'appelle « authentification à deux facteurs », ce qui signifie qu'il devra fournir des informations provenant d'au moins deux des trois catégories suivantes :

- **Un élément qu'il connaît** – comme un mot de passe ou un code PIN
- **Un élément qu'il possède** - comme un téléphone mobile, un lecteur de carte ou autre appareil
- **Un élément qu'il est** - comme un lecteur d'iris, la reconnaissance faciale ou une empreinte digitale

Annexe 4.2.2
Manuel du personnel

Voici un exemple d'un manuel du personnel qui présente la communication à votre personnel que nous recommanderions à propos de la SCA. Cette communication contient les informations de contexte nécessaires pour que vos collaborateurs puissent répondre à des questions courantes des clients, ce qui contribuera à éviter toute perturbation de votre activité.

Utilisez ces informations si votre entreprise offre des abonnements ou des paiements récurrents.

Comment les clients mettront-ils en place un nouvel abonnement ou paiement récurrent ?

Au moment de la création d'un nouvel abonnement, on demandera aux clients de confirmer leur identité selon la méthode d'authentification à deux facteurs choisie par leur banque. Les paiements subséquents et les abonnements existants n'exigeront pas l'authentification à deux facteurs, mais une authentification pourra être nécessaire si les clients apportent des modifications à leur abonnement.

Qu'est-ce que signifie la SCA pour nos clients ?

À partir du 14 septembre 2019, la manière dont vos clients paient en ligne pourra changer à cause de l'introduction de l'authentification à deux facteurs.

Les niveaux accrus de sécurité bénéficieront directement aux clients en renforçant leur confiance lors de leurs achats en ligne. Ils pourront aussi payer à partir de différents appareils tels que smartphones, tablettes et ordinateurs portables, pour une expérience client améliorée.

Dans le cadre de ces changements, les banques recevront plus de données afin de prendre des décisions mieux informées et d'évaluer si une transaction présente un risque faible (exemptée) ou si elle tombe hors du périmètre de la SCA. Ceci contribuera à créer une expérience de paiement fluide en réduisant le risque de fraude et le nombre de fois où les titulaires de cartes doivent authentifier leur paiement par carte Visa.

Que devons-nous faire ?

Nous devons tous nous informer à propos des changements qui seront introduits par la SCA pour pouvoir sensibiliser nos clients et les aider. Mais si ils ont des questions auxquelles vous ne pouvez pas répondre, veuillez les diriger d'abord vers leur banque émettrice, qui pourra fournir plus d'informations.

Annexe 4.2.2
Manuel du personnel

Voici un exemple d'un manuel du personnel qui présente la communication à votre personnel que nous recommanderions à propos de la SCA. Cette communication contient les informations de contexte nécessaires pour que vos collaborateurs puissent répondre à des questions courantes des clients, ce qui contribuera à éviter toute perturbation de votre activité.

FAQ

1. **Qu'est-ce que la SCA ?**
   SCA « Strong Customer Authentication » signifie « Authentification client forte ». À partir du 14 septembre 2019**,** les banques introduiront de nouvelles mesures de sécurité dans le cadre de nouvelles lois qui entreront en vigueur dans toute l'Europe pour les paiements par carte. Ces mesures rendront le paiement avec votre carte Visa encore plus sûr grâce à l'authentification à deux facteurs lorsque vous effectuez des paiements en ligne ou sans contact. Cela aidera les banques à s'assurer que c'est exclusivement le titulaire de carte qui paie avec sa carte Visa.

2. **Comment vos clients paieront-ils en ligne quand la SCA sera introduite ?**
   On pourra leur demander de franchir une étape de sécurité supplémentaire pour confirmer leur identité en utilisant la méthode d'authentification choisie par leur banque. Pour cela, ils devront fournir des informations provenant d'au moins deux des trois catégories ci-dessous :

- **Un élément qu'ils connaissent** – comme un mot de passe ou un code PIN
- **Un élément qu'ils possèdent** - comme un téléphone mobile, un lecteur de carte ou autre appareil
- **Un élément qu'ils sont** - comme un lecteur d'iris, la reconnaissance faciale ou une empreinte digitale

Annexe 4.2.2
Manuel du personnel

Voici un exemple d'un manuel du personnel qui présente la communication à votre personnel que nous recommanderions à propos de la SCA. Cette communication contient les informations de contexte nécessaires pour que vos collaborateurs puissent répondre à des questions courantes des clients, ce qui contribuera à éviter toute perturbation de votre activité.

Utilisez ces FAQ si votre entreprise offre des abonnements ou des paiements récurrents.

3. **Que se passera-t-il quand nos clients mettent en place un nouvel abonnement ou paiement récurrent ?**
   On pourra demander à nos clients de confirmer leur identité une seule fois au moment de la mise en place d'un nouvel abonnement ou paiement récurrent, en utilisant la méthode choisie par leur banque. Les paiements subséquents et les abonnements existants n'exigeront pas l'authentification à deux facteurs mais une authentification pourra être nécessaire si les clients apportent des modifications à leur abonnement.

4. **Que devront faire vos clients si leur transaction est refusée ou s'ils ne savent pas comment s'authentifier ?**
   Dites-leur de s'adresser à leur banque. La banque pourra les renseigner.

5. **Qu'est-ce que « Visa Secure » ?**
   Visa Secure est la technologie que les banques utilisent pour sécuriser les paiements de nos clients. Quand nos clients voient « Visa Secure » en ligne, ils peuvent être sûrs que leur transaction est protégée par plusieurs niveaux de sécurité. Ils sont également protégés par la politique de responsabilité zéro de Visa dans le cas où un tiers effectuerait une transaction frauduleuse avec leur carte Visa.

6. **Cette sécurité supplémentaire est-elle gratuite ?**
   Oui. Ce nouveau degré de protection est absolument gratuit pour les marchands Visa.

Annexe 4.3.1

Aide aux conversations

Voici un exemple d'une version plus concise du manuel destiné au personnel, qui présente la communication à votre personnel que nous recommanderions à propos de la SCA. Ce document peut être placé à côté des caisses en magasin pour aider les nouveaux employés qui n'ont pas encore suivi une formation.

À compter du 14 septembre 2019, les clients devront saisir leur code PIN de temps à autre lorsqu'ils effectuent des paiements sans contact.

Ces modifications de sécurité sont introduites afin de renforcer la protection des clients et de s'assurer que personne d'autre ne peut payer avec leur carte Visa.

Si la transaction sans contact d'un client exige une authentification, demandez-lui de saisir son code PIN pour finaliser son achat. Si la transaction est refusée, demandez-lui d'insérer sa carte et de saisir son code PIN pour effecteur un paiement puce + PIN. Si le problème persiste, demandez-lui de contacter sa banque émettrice qui pourra lui donner des informations complémentaires.

Annexe 4.3.2
Manuel du personnel

Voici un exemple de la communication à votre personnel que nous recommanderions à propos de la SCA. Cet exemple donne les informations de contexte et montre comment répondre à certaines questions courantes des clients.

Comment nos clients paient avec leur carte Visa en magasin
Les paiements de nos clients avec leur carte Visa en magasin seront bientôt encore plus sûrs et sécurisés.

À compter du 14 septembre 2019 de nouvelles mesures de sécurité seront introduites, appelées Authentification forte du client (Strong Customer Authentication, SCA). Ces changements ont pour but de fournir aux clients et entreprises une sécurité accrue et une meilleure protection contre la fraude lorsqu'ils effectuent et acceptent des paiements Visa.

Codes de réponse
Pour l'instant, quand notre fournisseur de service de paiement (PSP) traite la transaction d'un client, il envoie un code de réponse à 2 chiffres provenant de la banque émettrice pour nous dire si le paiement a été approuvé ou refusé, ou nous indiquer les mesures à prendre. Ces codes de réponse changeront après l'introduction de la SCA.

Comment les codes de réponse vont-ils changer ?
Pendant le processus de transaction, deux nouveaux codes de réponse seront activés dans les cas suivants :

- Si les clients effectuent plus de (5)** achats sans contact consécutifs depuis la dernière authentification forte, ou ;
- Si la valeur cumulée des paiements sans contact depuis la dernière authentification forte dépasse (150 €)** au total, ou ;
- Si un émetteur souhaite vérifier l'identité du client.

Annexe 4.3.2
Manuel du personnel

Voici un exemple de la communication à votre personnel que nous recommanderions à propos de la SCA. Cet exemple donne les informations de contexte et montre comment répondre à certaines questions courantes des clients.

Inclure ces informations dans les FAQ si elles sont pertinentes pour vos collaborateurs

Ce sont les banques qui contrôlent les nouveaux codes de réponse. Pour que notre entreprise soit prête le 14 septembre 2019, tous nos terminaux doivent être compatibles avec ces deux nouveaux codes :

1. **Code de réponse 70** – s'applique aux transactions PIN en ligne et demande au client de saisir son code PIN.
2. **Code de réponse 1A** – s'applique aux transactions PIN hors ligne et demande au terminal de changer d'interface pour l'insertion de la carte dans le terminal et la saisie d'un code PIN.

FAQ

1. **Qu'est-ce que la SCA ?**
   SCA signifie « Authentification client forte ». Les banques vont introduire de nouvelles mesures de sécurité dans le cadre de nouvelles lois qui entreront en vigueur dans toute l'Europe pour les paiements par carte. Ces mesures rendront le paiement avec votre carte Visa encore plus sûr grâce à l'authentification à deux facteurs pour les paiements sans contact. Cela aidera les banques à s'assurer que personne d'autre ne peut utiliser la carte Visa à part son titulaire.

2. **Que se passera-t-il quand les clients feront des achats en magasin et paieront sans contact ?**
   En magasin, on pourra leur demander de saisir leur code PIN plus souvent.

3. **Que doivent faire les clients si leur transaction sans contact est refusée ?**
   Il faut demander au client d'insérer sa carte et de saisir son code PIN pour effecteur un paiement par puce + PIN. Si la transaction échoue ou est refusée, vous devez demander au client de contacter sa banque émettrice. La banque pourra le renseigner.

*Insérer la date selon les besoins

Annexe 4.3.2
Manuel du personnel

Voici un exemple de la communication à votre personnel que nous recommanderions à propos de la SCA. Cet exemple donne les informations de contexte et montre comment répondre à certaines questions courantes des clients.

4. **Qu'est-ce que « Visa Secure » ?**
   Visa Secure est la technologie que les banques utilisent pour sécuriser les paiements des clients. Lorsqu'ils voient « Visa Secure » en ligne, ils peuvent être sûrs que leur transaction est protégée par plusieurs niveaux de sécurité.

5. **Comment Visa protège-t-il les clients ?**
   Ils sont protégés par la politique de responsabilité zéro de Visa dans le cas où un tiers effectuerait une transaction frauduleuse avec leur carte Visa.

6. **Cette sécurité supplémentaire est-elle gratuite ?**
   Oui. Ce nouveau degré de protection est absolument gratuit pour les marchands Visa.

Si vous êtes marchand et avez à la fois des activités en ligne et hors ligne, combinez ces informations selon les besoins.

Merci