ASSOCIATION DU PAIEMENT
Les acteurs français des services du paiement électronique

NOTE DE REFLEXION ASSOCIATION DU PAIEMENT
GENEROSITE AU POINT DE VENTE OU EN LIBRE-SERVICE

Paris, le 3 Octobre 2019

Dans le cadre de sa mission d'analyse du marché, l'Association du Paiement suit depuis maintenant plusieurs mois le déploiement et la commercialisation des solutions permettant de faire de la générosité au point de vente, via un équipement monétique.

Cette note de vulgarisation a été émise par l'Association du Paiement pour rappeler le contexte, les différents modes de fonctionnement, les bonnes pratiques en la matière, les risques liés et la réglementation associée. Elle pourra être utilisée par les concepteurs, les distributeurs et les acheteurs dans le cadre de leur développement, ou les utilisateurs pour s'assurer de la conformité et de la sécurité de la solution utilisée.

PREAMBULE – RAPPEL

Le consommateur français est maintenant habitué, depuis de très nombreuses années, à utiliser sa carte bancaire, dans un environnement de sécurité très satisfaisant. En effet, depuis le développement des solutions, l'écosystème en place (avec notamment le GIE Carte Bancaire, les acquéreurs, les émetteurs et les industriels) a mis en place des solutions fiables, sécurisées, en complément des solutions de lutte contre la fraude. C'est grâce à tous ces efforts que la fraude à la carte atteint des niveaux « à minima ».

Le but de cette note de réflexion n'est pas de revenir sur les effets de la fraude à la carte bancaire : d'autres publications spécialisées se sont déjà fait l'écho de ce phénomène, des effets et des risques liées (La Banque de France a notamment émis des recommandations consultables sur son site[1]). Par contre, elle souhaite revenir sur les règles de sécurité à mettre en place, l'environnement technique à disposition et la réglementation à appliquer

LE TERMINAL DE PAIEMENT UTILISE

Les différentes solutions mises en place et expérimentations réalisées peuvent être classées en deux catégories :

- **La générosité sur le terminal de paiement** : c'est lors de son passage en magasin que le consommateur peut, s'il le souhaite, rajouter une somme spécifique (montant fixe, arrondi ou pourcentage de la transaction) à sa transaction de paiement. C'est le terminal de paiement qui gère de bout en bout la transaction, la valide et procède à la remontée des informations sur l'environnement de compensation.
- **La générosité sur une borne autonome** : la borne est en libre-service, sans intervention directe du commerçant lors de l'acte de générosité. Elle n'est donc pas surveillée en permanence et doit être soumises à des normes de sécurité spécifiques. Le porteur doit/peut faire son choix du montant parmi un ensemble de sommes proposées par l'application de générosité embarquée sur la borne ou sur un écran déporté. Dans tous les cas, il ne peut/doit interagir (« prendre la main ») sur cette application. Comme dans l'environnement précédent, c'est la borne qui gère de bout en bout la transaction, la valide et procède à la remontée des informations sur l'environnement de compensation.

[1] https://www.banque-france.fr/stabilite-financiere/observatoire-de-la-securite-des-moyens-de-paiement

Dans les deux solutions présentées ci-dessus, l'application développée doit s'appuyer sur les règles du paiement en mode « proximité » ou en mode « automate » qui seules permettent au donateur d'être authentifié et donc au commerçant de bénéficier d'un transfert de responsabilité qui lui garantit d'être réglé in-fine. Les autres solutions peuvent, faute de garanties ou de sécurité poussées, présenter un risque important pour le commerçant : sans transfert de responsabilité, il n'y a pas de garantie et il peut ne pas être réglé.

Quelle que soit la solution retenue par l'offreur de service, le terminal utilisé pour héberger l'application de générosité, doit être agréée. Il doit donc avoir subi (et réussi) les différents tests mis en place. On peut notamment citer (sans que cette liste soit totalement exhaustive) les tests réalisés par EMV (pour l'ensemble des Pays) et ceux menés par le (ou les) Schéma(s) de paiement que le marchand veut pouvoir accepter : CB pour les Cartes Bancaires françaises, Visa, Mastercard, JCB, Discover, UPi, American Express (pour les cartes étrangères).

LA SECURITE DU PORTEUR

Quelle que soit la transaction réalisée, ainsi que la solution retenue, quelques règles de sécurité doivent être strictement respectées. Sans toutes les citer, on peut notamment rappeler que le porteur doit effectuer son paiement de façon automatique, sans avoir à indiquer manuellement les informations de sa carte sur l'application de générosité : lecture en mode « puce » (contact/sans contact) ou piste. Si le porteur devait saisir son numéro de carte, ceci doit être fait sur un device (terminal) lui appartenant (son smartphone par exemple) et non sur la borne ou sur le device du commerçant. En effet, tout doit être mis en œuvre pour éviter que les informations saisies ne puissent être détournées.

Le transfert, la conservation et le traitement des données doivent être réalisés selon des règles strictes de sécurité, inhérentes aux moyens de paiement. Les environnements doivent donc être notamment conformes au standard PCI-DSS les plus récents.

L'ENVIRONNEMENT BANCAIRE UTILISE

De façon à traiter les flux dans les meilleurs conditions de sécurité et de respect des réglementations, la solution retenue doit faire l'objet d'un avis favorable des institutions de contrôles de son pays (telles que la Banque de France et/ou l'Autorité de Contrôle Prudentiel et de Résolution, pour la France).

Elle doit s'appuyer sur des établissements financiers reconnus, si possible Européen (banque, établissement de paiement, émetteur de monnaie électronique).

Le pays ou est traité le flux doit être un point d'attention particulier.

POUR TERMINER

L'Association du Paiement a souhaité émettre cette note de vulgarisation dans un souci d'éclairage du marché. Bien sûr, la sécurité a un coût mais, lorsque les conditions listées précédemment ne sont pas toutes mises en œuvre, le commerçant doit savoir que c'est son image de marque qui pourrait en pâtir, si la fraude augmente. Il devra donc s'attacher à vérifier que les solutions qui lui sont proposées respectent bien les conditions énoncées ci-dessus.