- PUBLIC -

Observatoire de la sécurité des moyens de paiement
www.observatoire-paiements.fr

Paris, le 7 juin 2024

L'Observatoire de la sécurité des moyens de paiement lance un plan de renforcement de la sécurité des paiements par carte à distance

De quoi parle-t-on ?

Les paiements par carte à distance se décomposent en trois grandes catégories :

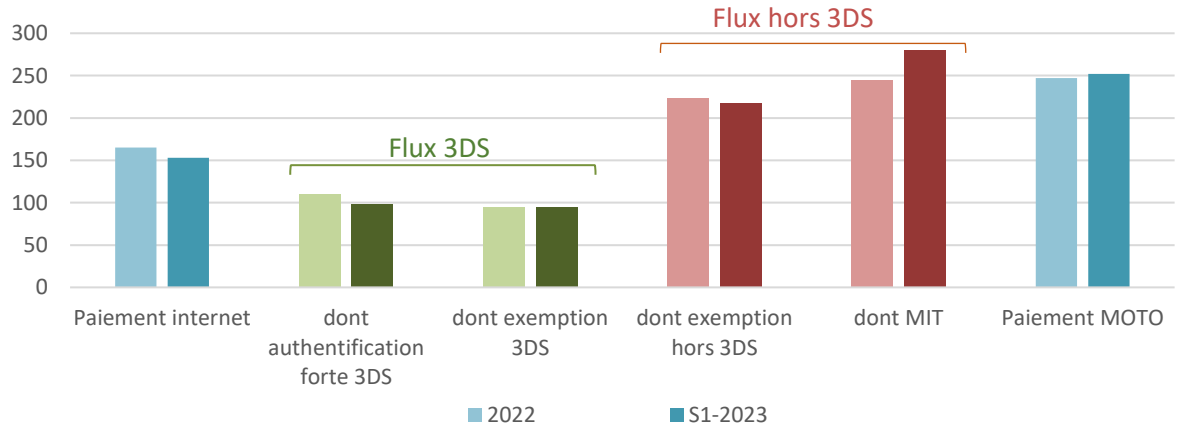
- Les paiements directs sur internet (ou CIT pour *Customer Initiated Transaction*), qui correspondent aux paiements unitaires réalisés au moment d'un achat sur un site d'e-commerce. La réglementation impose le recours à une authentification forte au moment du paiement, sauf si celui-ci relève de l'un des cas d'exemption définis dans la réglementation en raison d'un niveau de risque limité (par exemple pour les paiements de faible montant).
- Les paiements différés sur internet (ou MIT pour *Merchant Initiated Transaction*), qui correspondent à des paiements consécutifs à un engagement à payer pris lors de la souscription sur un site d'e-commerce, par exemple dans le cas d'un abonnement périodique, d'un paiement en plusieurs fois, ou encore d'un paiement ajusté en fonction de la consommation de l'utilisateur. Dans ce cas de figure, l'authentification forte a lieu au moment de la souscription, les paiements étant émis par le commerçant sans nouvelle intervention de son client (à l'image d'un prélèvement automatique).
- Les paiements à distance hors internet (ou MOTO pour *mail order / telephone order*) correspondent à des paiements réalisés au moyen d'un moyen de communication non automatisé : transmission d'une commande sur un bordereau papier (courrier ou télécopie) ou insérée dans un courriel, ou encore commande passée par téléphone. Dans ce cas de figure, le client fournit les informations relatives à sa carte de paiement au commerçant, qui se charge de les saisir ensuite dans l'interface de paiement.

Par ailleurs, une partie des paiements sur internet s'appuient sur un protocole technique appelé *3-D Secure*, permettant d'assurer une mise en relation entre le commerçant, le consommateur et la banque de celui-ci, afin de permettre soit de procéder à l'authentification forte du client, soit de communiquer à la banque des informations permettant à celle-ci d'accorder le cas échéant une exemption à l'authentification forte. Le recours à ce protocole ne revêt toutefois pas de caractère obligatoire : certains paiements sur internet peuvent ainsi être authentifiés directement par la banque (c'est le cas quand le client utilise certains portefeuilles électroniques mobiles) ou bénéficier d'une exemption (pratique dite de DTA pour *Direct to Authorisation*).

Quels sont les paiements à distance les plus vulnérables aujourd'hui ?

Depuis la mise en place de l'authentification forte des paiements électronique issue de la 2e directive européenne sur les services de paiements (ou DSP2), l'Observatoire de la sécurité des moyens de paiement note que les paiements à distance sans authentification forte réalisés en-dehors du protocole *3-D Secure*, qu'il s'agisse de flux de type CIT, MIT ou MOTO, présentent structurellement des taux de fraude plus de deux fois supérieurs à ceux des paiements sur internet avec authentification forte et/ou s'appuyant sur le protocole technique *3-D Secure*.

Graphique : taux de fraude sur les paiements par carte à distance
(en € de fraude / 100.000 € de paiements)



Source : Observatoire de la Sécurité des Moyens de paiement

En quoi consiste le plan d'actions adopté par l'Observatoire ?

Le plan d'actions de l'Observatoire vise à limiter les paiements à distance sans authentification forte réalisés en-dehors du protocole *3-D Secure*, plus exposés à la fraude, et à favoriser le recours aux canaux les plus sécurisés, notamment au protocole technique *3-D Secure*. Il s'appuie sur le plafonnement par les banques émettrices des usages identifiés comme risqués sur la base de la mesure de la « vélocité », un indicateur qui mesure le montant total des paiements réalisés avec une carte au cours des dernières 24 heures auprès d'un commerçant :

- Si une transaction conduit à dépasser le seuil de vélocité fixé, alors la banque du porteur rejettera cette transaction en invitant le commerçant à recourir à un autre canal de paiement, sauf si le commerçant relève d'un secteur d'activité pour lequel le type de transaction est jugé incontournable et peu fraudé (cas en particulier des secteurs du voyage, de la vente sur catalogue et du recouvrement de créances pour les paiements MOTO) – la liste des activités ainsi exclues de la limitation de vélocité est jointe au plan d'actions et pourra être révisée si besoin ;
- La vélocité sera calculée séparément pour les paiements MOTO d'une part, et pour les paiements internet hors *3-D Secure* d'autre part : concernant spécifiquement les paiements MIT, les banques pourront les intégrer au périmètre des flux couverts par ce mécanisme de plafonnement au cas par cas, dès lors que la preuve d'authentification forte initiale (ou « chainage ») présentée par le commerçant sera jugée invalide ;
- Le seuil de vélocité sera initialement fixé à 500 € au démarrage du plan, le 10 juin 2024 ; il sera ensuite abaissé à 250 € à la rentrée 2024, puis à 100 € au dernier trimestre 2024.

L'Observatoire assurera un pilotage continu de la mise en place de ce plan et de ses conséquences sur la fraude et sur le bon fonctionnement du e-commerce. En particulier, avant chaque abaissement de ce seuil, il s'assurera que le marché français est suffisamment prêt à l'absorber, et pourra être amené à ajuster la liste des secteurs exclus de l'application de ces mesures en cas de besoin.

La mise en application pratique des mesures

Exemples de cas de figure concernés par la limite de vélocité

Monsieur X. fait ses achats en ligne sur un grand site de e-commerce généraliste, où il a pris l'habitude de faire appel au service client du site par téléphone au moment du paiement, pour ne pas avoir à saisir son numéro de carte sur internet ni à utiliser le système d'authentification forte mis à sa disposition par sa banque ; il préfère confier son numéro de carte à un opérateur, qui règle ensuite la transaction par saisie du numéro de carte sur son terminal (c'est un paiement de type MOTO).

⇨ Cette pratique du site de e-commerce comporte un risque de fraude par détournement du numéro de carte de Monsieur X. Ce cas d'usage n'est donc pas légitime, le site de e-commerce doit inviter Monsieur X. à régler ses achats directement en ligne via le protocole *3-D Secure*, qui permet notamment d'assurer un haut niveau de sécurité des données de paiement échangées. Les paiements effectués par téléphone seront astreints à la limite de vélocité.

Pour ses prochaines vacances, Madame Y. commande sur internet un voyage pour un montant total de 2 100 euros. Compte tenu du montant de cet achat, elle choisit un paiement fractionné en 4 fois.

⇨ Pour garantir la sécurité des paiements, l'agence de voyages en ligne doit exiger une authentification forte lors de la commande du voyage, portant sur le montant total. À défaut, les paiements, d'un montant unitaire supérieur au plafond de 500 euros applicable à compter du 10 juin 2024, pourront être rejetés.

Exemples de cas de figure non concernés par la limite de vélocité

Depuis plusieurs années, Monsieur Z. réalise un don mensuel de 150 euros à une association caritative. Ce montant est débité chaque mois de sa carte bancaire, dont Monsieur Z. avait renseigné le numéro sur le site internet de l'association (paiement MIT).

⇨ L'association continuera de bénéficier de la générosité de Monsieur Z., même lorsque la limite de vélocité aura été abaissée à 100 euros. En effet, pour les paiements MIT, les œuvres sociales et caritatives sont exemptées des mesures adoptées par l'Observatoire.

Madame K. a reçu de son fournisseur d'énergie une facture de régularisation d'un montant élevé. À la date prévue pour le prélèvement automatique, le solde du compte bancaire de Madame K. n'était pas suffisant pour permettre au prélèvement d'être accepté. Après avoir alimenté son compte bancaire, Madame K. appelle le service clients de son fournisseur d'énergie pour régulariser sa situation en payant par carte bancaire. Madame K. est invitée à saisir le numéro de sa carte directement sur le clavier de son téléphone.

⇨ La pratique du fournisseur d'énergie (saisie du numéro de carte sur le clavier du téléphone) est conforme aux recommandations de l'Observatoire et le secteur d'activité concerné est exempté de la limitation de la vélocité pour les paiements MOTO, en raison à la fois d'un niveau de fraude

très faible et du besoin de maintenir ce mode de règlement pour des populations ne maitrisant pas suffisamment internet pour procéder à une régularisation d'urgence en ligne.

Modalités d'application de la vélocité

Exemples donnés dans le cas d'une limite fixée à 250 euros (période de septembre à octobre 2024) :

- Le client réalise auprès d'une même enseigne un paiement non authentifié émis par le commerçant en-dehors de *3-D Secure* de 240 euros et un paiement MOTO de 120 euros : les deux paiements pourront être acceptés, car la vélocité est mesurée séparément pour chaque catégorie de paiements.
- Auprès du même commerçant et pendant la même journée, le client réalise deux paiements MOTO de 120 euros chacun, puis souhaite réaliser un 3ème paiement MOTO d'un montant de 20 euros : ce 3ème paiement sera rejeté car il conduirait au dépassement du plafond de 250 euros.
- Le client tente d'effectuer un 1er paiement MOTO d'un montant de 300 euros auprès d'un commerçant n'appartenant pas à un secteur d'activité exempté : le paiement sera rejeté car il conduirait à lui seul au dépassement du plafond.