**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Statistiques de fraude des systèmes de paiement par carte

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Collecte de l’Observatoire de la sécurité des moyens de paiement

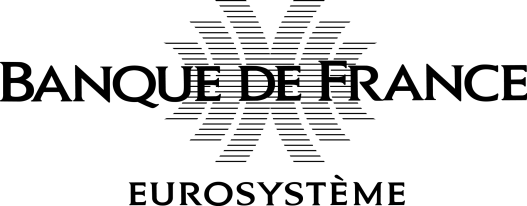
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Guide de remplissage**

à l’attention des déclarants

**Applicable à partir des données**

**du 1er semestre 2023**



**Suivi des versions**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Commentaires** |
| 0.5 | 17/12/2020 |  |
| 0.6 | 14/01/2022 | Ajout de 4 sous composantes à l’indicateur « Dont paiements non authentifiés » pour les paiements sur Internet. |
| 0.7 | 15/02/2022 | Correction de la définition du paiement « *one leg* » et complément de la définition de « Dont paiements 3D Secure sans authentification forte ». |
| 0.8 | 22/05/2023 | i) Exclusion des données de cartes de monnaie électronique de la collecte  ii) Précisions de la définition relative au dénombrement des supports autre que carte  iii) Ajout de la catégorie « dont paiements hors 3D Secure avec authentification forte »  iv) Précisions des définitions de « paiements 3D Secure avec authentification forte », « paiements non 3DS non conformes à la DSP2 » et « paiements non authentifiés »  v) Rajout de la Guyane française dans l’annexe partie zones géographiques/zone France |

**Avant-propos**

Le guide de remplissage de la collecte de l’OSMP prend en compte les orientations de l’ABE existantes depuis le 1er janvier 2021 auprès des prestataires de service de paiement français. Les principaux changements apportés à la collecte par ce texte ont été :

* La périodicité de la collecte est devenue semestrielle ;
* La ventilation géographique des données se fait selon les zones : France, zone de l’Espace Économique et Européen (EEE) et zone hors de l’EEE ;
* Les modes d’authentification des transactions par carte sont suivis.

**1. Introduction**

En vertu des articles L. 141-4 et R. 141-1 du Code monétaire et financier, l’Observatoire de la sécurité des moyens de paiement est chargé d’établir des statistiques de fraude harmonisées pour les moyens de paiement en vue de leur publication au sein de son rapport annuel disponible à l’adresse suivante : <https://www.banque-france.fr/liste-chronologique/rapports-dactivite>.

 À cette fin et pour ce qui concerne la carte de paiement, la Banque de France pour le compte du secrétariat de l’Observatoire recueille les données permettant l’évaluation de la fraude auprès des déclarants que sont :

* Les systèmes de paiement par carte interbancaires nationaux et internationaux opérant en France pour ce qui concerne les opérations réalisées par leurs membres ;
* Et, les émetteurs de cartes privatives nationaux et internationaux actifs en France.

Ce guide de remplissage fournit aux déclarants toutes les informations nécessaires pour répondre à cette collecte. Un glossaire sur les termes utilisés dans le guide est situé en annexe.

☞Remarque aux établissements émettant à la fois des cartes privatives et interbancaires : seules les données relatives aux cartes privatives doivent être déclarées, celles concernant les cartes interbancaires devant être transmises par les gestionnaires des systèmes interbancaires concernés.

**2. Présentation de la collecte**

* ***Nature des données* collectées** : elles portent sur le nombre et le montant des transactions frauduleuses ainsi que sur le nombre et le montant total des transactions dans le but de calculer les taux de fraude. Les transactions concernées sont toutes les transactions de paiement (de proximité et à distance) et de retrait effectuées par carte de paiement et réalisées en France et à l’étranger **dès lors que l’une des contreparties de la transaction est considérée comme française** : carte émise par un établissement français ou transaction acceptée en France (commerçant établi en France ou DAB/GAB installé en France). Les données de cartes de monnaie électronique, donc les cartes prépayées, sont dorénavant exclues de la collecte.
* ***Présentation des données collectées***: les données en volume doivent être déclarées en unités et celles exprimées en valeur en euros. Si les données sources sont dans une autre devise, il convient de les convertir en euros en utilisant de préférence les taux de change publiés par la BCE (*ww.ecb.int, Euro foreign exchange reference rates*). Il est précisé que la BCE publie les taux de conversion pour chaque jour ouvré du calendrier ainsi que des moyennes mensuelles, trimestrielles et semestrielles.
* ***Date de référence des données collectées :*** il convient de retenir la date d’exécution de l’opération frauduleuse et non la date à laquelle la fraude a été découverte/déclarée ou celle à laquelle le vol de la carte ou des données de carte a eu lieu.
* ***Zones géographiques de la collecte*** : les données de transaction et de fraude sont à ventiler en trois zones géographiques distinctes : « France », « Étranger au sein de l’EEE » (hors France) et « Étranger hors EEE ». Cette ventilation s’opère en fonction des pays où sont établis respectivement l’émetteur de la carte et l’accepteur de la transaction (commerçant ou DAB/GAB), **sans chevauchement**, pour éviter les doubles comptes des transactions et de la fraude. Les périmètres des zones France et EEE sont précisés en annexe.
* ***Évaluation de la fraude :***
  + ***Définition de la fraude :***

|  |
| --- |
| La fraude est définie comme l’utilisation illégitime d’une carte de paiement ou des données qui lui sont attachées, ainsi que tout acte concourant à la préparation ou à la réalisation d’une telle utilisation :   * **ayant pour conséquence un préjudice financier :** pour l’établissement teneur de compte qu’il s’agisse du banquier du porteur de la carte ou de celui de l’accepteur (commerçant, administration… pour son propre compte ou au sein d’un système de paiement), le porteur, l’accepteur, l’émetteur, un assureur, un tiers de confiance ou tout intervenant dans la chaîne de conception, de fabrication, de transport, de distribution de données physiques ou logiques, dont la responsabilité civile, commerciale ou pénale pourrait être engagée ; * **quel que soit le mode opératoire retenu :**   + les moyens employés pour récupérer, sans motif légitime, les données ou le support de la carte (vol, détournement du support de la carte, des données physiques ou logiques, des données de personnalisation et/ou récupération du code secret, et/ou du cryptogramme, piratage de la piste magnétique et/ou de la puce…) ;   + les modalités d’utilisation de la carte ou des données qui lui sont attachées (paiement/retrait en situation de proximité ou à distance, par utilisation physique de la carte ou du numéro de carte, sur automate…) ;   + la zone géographique d’émission ou d’utilisation de la carte ou des données qui lui sont attachées ;   + le type de carte de paiement ; * **et, quelle que soit l’identité du fraudeur** : un tiers, le banquier teneur de compte, le porteur de la carte lui-même (dans le cas par exemple d’une utilisation après déclaration de vol ou de perte, ou d’une dénonciation abusive de transactions), l’accepteur, l’émetteur, un assureur, un tiers de confiance, etc. |

* + ***Approche « fraude brute » :*** la fraude doit être évaluée selon cette approche (par opposition à l’approche « fraude nette ») qui consiste à prendre en compte (i) l’ensemble des transactions autorisées (ii) ayant ensuite fait l’objet d’un rejet a posteriori pour motif de fraude et (iii) pour leur montant initial sans prise en compte des mesures prises ultérieurement par les contreparties en vue de réduire le préjudice. Les tentatives de fraude ou « fraude déjouée » (fraude stoppée avant exécution de l’opération) sont à exclure de la déclaration.

**3. Calendrier et communication de la collecte**

* ***Calendrier****:* la collecte est semestrielle et les périodes de collecte s’étendent pour les données :
* Du premier semestre (période de janvier à juin) du 1er jour ouvrable d’août au dernier ouvrable d’octobre ;
* Du second semestre (période de juillet à décembre) du 1er jour ouvrable de février au dernier jour ouvrable d’avril.

Les déclarants sont informés de l’ouverture des collectes directement par le secrétariat de l’OSMP.

* ***Modalités de déclaration*** : la déclaration s’effectue au travers du portail OneGate – Oscamps (portail de collecte de la Banque de France) dont les modalités d’accès sont précisées dans le manuel utilisateur externe ONEGATE.

Un contrat d’interface remettant complète le présent guide de remplissage.

L’ensemble de la documentation technique est disponible sur le site internet de la Banque de France à l’adresse suivante : [Collecte pour le compte de l'Observatoire de la sécurité des moyens de paiement | Banque de France (banque-france.fr)](https://www.banque-france.fr/stabilite-financiere/securite-des-moyens-de-paiement-scripturaux/collectes-statistiques-reglementaires-espace-declarants/collecte-pour-le-compte-de-lobservatoire-de-la-securite-des-moyens-de-paiement)

Une version Excel du questionnaire est disponible via ce fichier :



**Pour toute information vous pouvez contacter le service de la Banque de France en charge d’assurer le secrétariat de l’OSMP dont les coordonnées suivantes :**

|  |
| --- |
| DIRECTION GENERALE DES MOYENS DE PAIEMENT  Direction des études et surveillance des paiements  Service de la Surveillance des Moyens de Paiement Scripturaux  S2B-2323  75049 PARIS CEDEX 01  [2323-OSMP-UT@banque-france.fr](mailto:2323-OSMP-UT@banque-france.fr). |

**4. Structure et contenu du questionnaire**

La structure du questionnaire se présente comme suit :

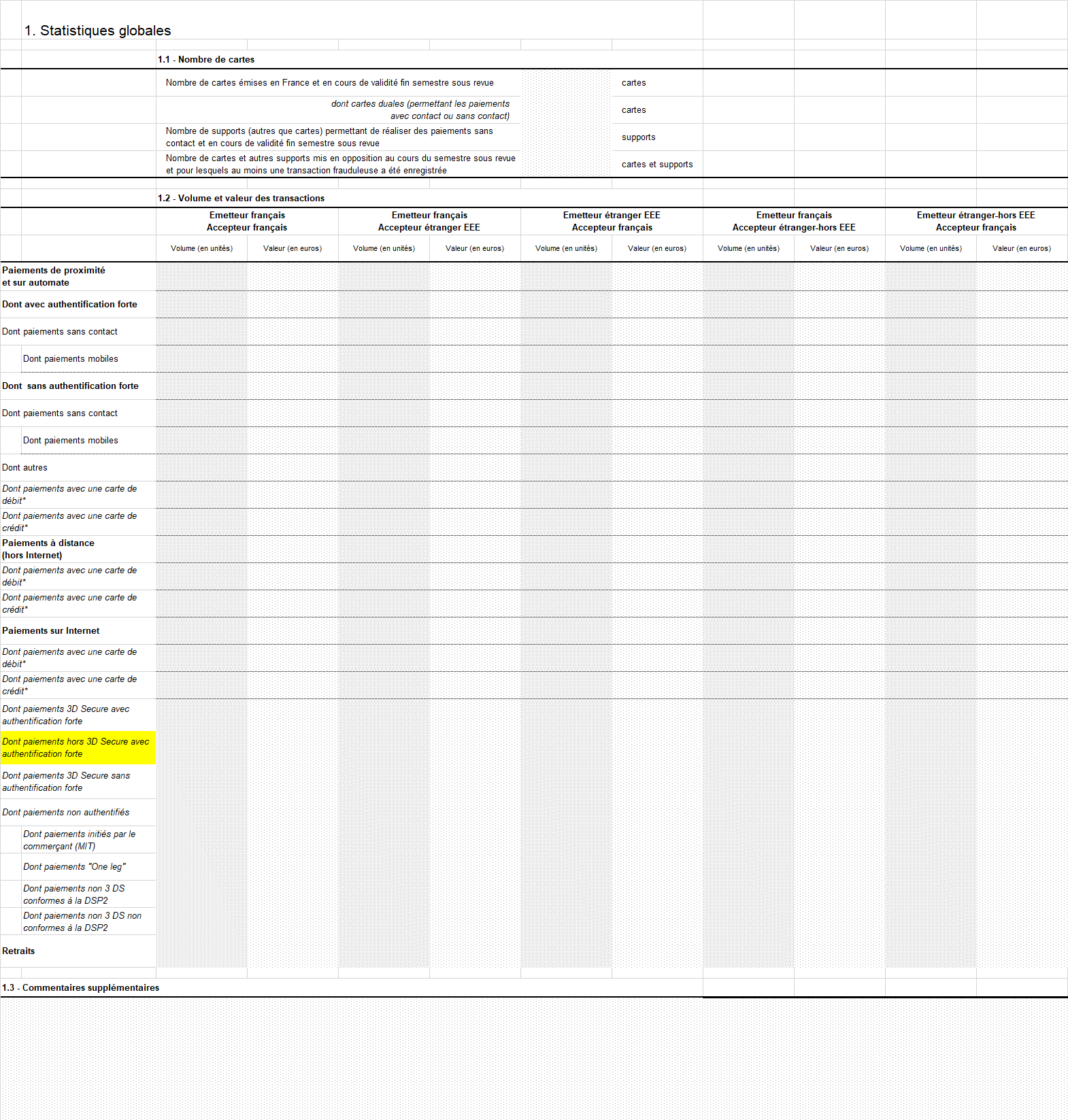
* Section 1.1 – Nombre de cartes : recense les données sur les volumes des cartes en circulation et mises en opposition.
* Section 1.2 – Volume et valeur des transactions : recense le nombre et le montant des transactions ventilés par type de transaction, par mode d’authentification et par zone géographique de l’émetteur de la carte et de l’accepteur de la transaction.
* Sections 2.a à 2.e – Répartition de la fraude : origine de la fraude : pour chaque zone géographique de l’émetteur de la carte et de l’accepteur de la transaction, recense le nombre et le montant des transactions frauduleuses ventilés par type de transaction, mode d’authentification, par fonction de la carte et par typologie de fraude.
* Section 3.1 – Ventilation de la fraude en vente à distance par secteur d’activité sur les transactions nationales : recense la fraude nationale sur les paiements à distance selon le secteur d’activité du commerçant.

**Section 1.1 - Nombre de cartes**

|  |  |  |
| --- | --- | --- |
| **1.1 - Nombre de cartes** | | |
| Nombre de cartes émises en France et en cours de validité fin semestre sous revue |  | cartes |
| *dont cartes duales (permettant les paiements avec contact ou sans contact)* |  | cartes |
| Nombre de supports (autres que cartes, tels que les smartphones, les montres ou les objets connectés) permettant de réaliser des paiements par carte en mode sans contact et en cours de validité à la fin du semestre sous revue. La comptabilisation des *tokens* associés à de tels supports peut servir de base d’estimation pour cet indicateur. |  | supports |
| Nombre de cartes et autres supports mis en opposition au cours du semestre sous revue et pour lesquels au moins une transaction frauduleuse a été enregistrée |  | cartes et supports |

* **Cartes de paiement:** Sont à exclure les cartes qui ne sont pas habilitées aux paiements et qui permettent de faire des retraits uniquement sur les GAB/DAB de l’établissement qui les a émises, ainsi que les cartes émises sous le régime réglementaire de la monnaie électronique.
* **Règles spécifiques devant être appliquées pour les établissements émettant des cartes co-badgées (CB-MasterCard ou CB-Visa) et destinées à prévenir les doubles comptes ou les omissions :**
* **Par le GIE CB** : toutes les cartes « CB », y compris celles co-badgées CB-MasterCard ou CB-Visa doivent être déclarées dans la section 1.1 ;
* **Par MasterCard et Visa** : seules les cartes « MasterCard Only » ou « Visa Only » doivent être déclarées dans la section 1.1 ; les cartes co-badgées CB-MasterCard ou CB-Visa sont donc à exclure.

**Section 1.2 - Volume et valeur des transactions**



* **Type de transaction :**

|  |  |
| --- | --- |
| **Paiements de proximité et sur automate** | Paiements réalisés au point de vente ou sur automate, y compris le paiement en mode sans contact |
| Dont paiements avec authentification forte | Paiements de proximité par carte pour lesquels une authentification forte du client a eu lieu. Par exemple, paiements en mode « chip&PIN », avec vérification du PIN en ligne (PIN Online), par carte biométrique ou par téléphone mobile avec lecture d’une empreinte biométrique, saisie d’un mPIN ou d’un mot de passe. |
| Dont paiements sans authentification forte | Paiements de proximité par carte pour lesquels il n’y a pas eu d’authentification forte, par exemple carte à piste ou à puce avec signature manuscrite, carte en mode sans contact sans vérification d’empreinte biométrique ou du PIN en ligne (PIN Online), ou par téléphone mobile sans facteur d’authentification d’inhérence (lecture d’une empreinte biométrique) ou de connaissance (mot de passe). |
| Dont paiements sans contact | Paiements de proximité en mode sans contact |
| Dont paiements mobiles | Paiements de proximité dans lesquels un appareil mobile (téléphone, tablette, montre connectée…) est utilisé pour initier un ordre de paiement par une technologie sans contact (par exemple : NFC, Bluetooth, code barre à 1 ou 2 dimensions) et éventuellement pour le transfert de fonds. Parmi les offres les plus connues, citons par exemple, Apple Pay, Samsung Pay, Google Pay, Lyf, Paylib sans contact.  💣 Les « paiements mobiles » sont un sous-ensemble de « paiements sans contact » |
| Dont autres | Paiements sur automates de parking ou d'autoroute, par exemple, avec lecture de la piste magnétique de la carte |
| **Paiements à distance (hors internet)** | Paiements réalisés par courrier, postal ou électronique (courriel), ou par fax/téléphone (ou MOTO) |
| **Paiements sur internet** | Paiements réalisés sur Internet (site commerçant ou via application) |
| Dont paiements 3D Secure avec authentification forte | Paiements réalisés sur Internet au travers de l’infrastructure 3D-Secure avec une authentification forte du porteur (*customer initiated transaction – CIT).* Cela peut inclure certains paiements où l’authentification forte a été déléguée à un tiers de l’émetteur en conformité avec les règles d’externalisation applicables dans le cadre de la DSP2 (ex : portefeuille mobile de type X-Pay proposé sous la responsabilité de l’émetteur, délégation de l’authentification forte auprès du commerçant sous la responsabilité de l’émetteur etc.). |
| Dont paiements hors 3D Secure avec authentification forte | Paiements internet, sans passer par les infrastructures 3D-Secure, où l’authentification forte a été déléguée à un tiers en conformité avec les règles d’externalisation applicables dans le cadre de la DSP2 (ex : portefeuille mobile de type X-Pay proposé sous la responsabilité de l’émetteur, délégation de l’authentification forte auprès du commerçant sous la responsabilité de l’émetteur etc.). |
| Dont paiements 3D Secure sans authentification forte | Paiements réalisés sur Internet au travers de l’infrastructure 3D-Secure sans authentification forte du porteur c’est-à-dire en appliquant une exemption prévue par les RTS (transactions dites « *frictionless*»)ou en cas d’incident technique ne permettant pas de la mettre en œuvre. Les authentifications mono-facteur (ex : SMS-OTP seul) sont également à reprendre dans cette ligne. |
| Dont paiements non authentifiés | Tous les paiements sur Internet réalisés n’ayant été soumis ni aux infrastructures 3-D Secure ni à une authentification forte. |
| Dont paiements initiés par le commerçant (MIT) | Paiements initiés par le commerçant sans présence active du porteur de la carte sur la base d’un accord préexistant (« mandat MIT ») comme par exemple, un abonnement, un paiement en plusieurs fois, un service payé en fonction de la consommation. Dans le cas d’un paiement à la fois « MIT » et « *one leg* », le paiement doit être considéré comme « MIT ». |
| Dont paiements « *one leg* » | Paiements hors 3D-Secure pour lesquels l’émetteur de la carte ou l’accepteur du paiement n’est pas localisé dans l’Espace économique européen. |
| Dont paiements non 3DS conformes à la DSP2 | Paiements présentant un facteur d’exemption (ex *: Direct to Authorization* – DTA avec présence d’un facteur d’exemption dans le flux d’autorisation). |
| Dont paiements non 3DS non conformes à la DSP2 | Paiements entrant dans le périmètre d’application de la DSP2, initiés par le porteur (*customer initiated transaction* – CIT) qui vont directement en autorisation sans facteur d’exemption. Les paiements qui impliquent un accepteur européen et un acquéreur non-européen (hors EEE) sont également à reprendre dans cette ligne. Dans le cas d’un paiement à la fois «*one leg* » et «non 3DS non conformes à la DSP2 » , le paiement doit être considéré comme « *one leg* ». |
| **Retraits** | Retraits d’espèces à un distributeur de billets |

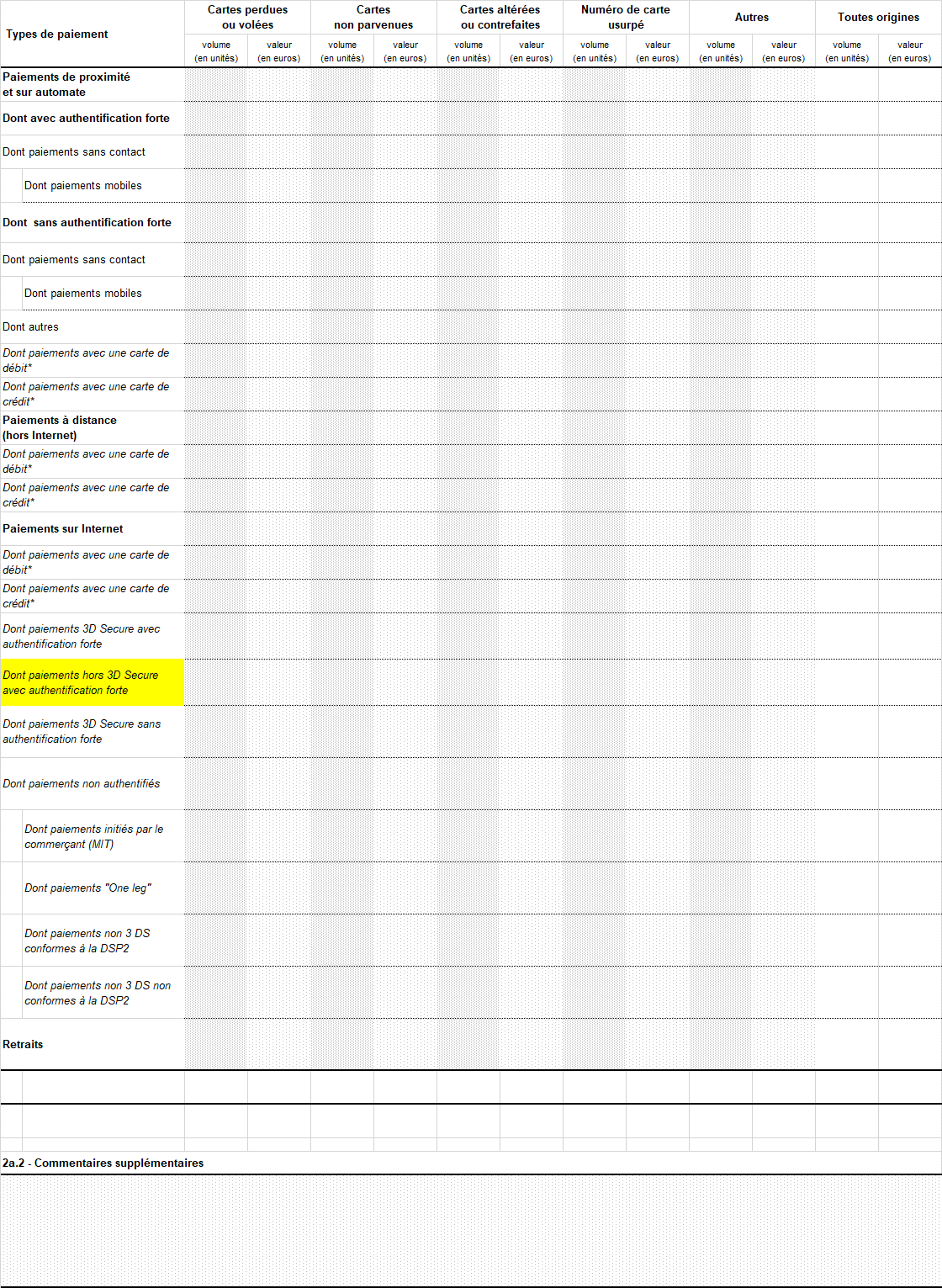
* **Type de carte :**

|  |  |
| --- | --- |
| Carte de débit | Carte à débit immédiat |
| Carte de crédit | Carte de crédit et carte à débit différé |

Remarque : pour les cartes commerciales, si l’établissement n’est pas en capacité de connaitre la fonction de carte, par défaut il les ventile dans la rubrique « carte de crédit ».

* **Règles spécifiques devant être appliquées pour les établissements émettant des cartes co-badgées (CB-MasterCard ou CB-Visa) et destinées à prévenir les doubles comptes ou les omissions :**
* **Par le GIE CB** : ne déclarer que les transactions traitées par le système « CB » (indépendamment du fait que la carte utilisée soit une carte « CB only » ou une carte co-badgée) ;
* **Par MasterCard et Visa** : ne déclarer que les transactions traitées[[1]](#footnote-1) par le système MasterCard ou le système Visa (indépendamment du fait que la carte utilisée soit une carte « MasterCard Only », « Visa only » ou une carte co-badgée.

**Sections 2.a.1 à 2.e.1 - Répartition de la fraude**



* **Origine de la fraude :**

|  |  |
| --- | --- |
| Carte perdue ou volée | Le fraudeur utilise une carte de paiement à la suite d’une perte ou d’un vol, à l’insu du titulaire légitime |
| Carte non parvenue | La carte a été interceptée lors de son envoi par l’émetteur à son titulaire légitime. Ce type de fraude se rapproche de la perte ou du vol. Cependant, il s’en distingue, dans la mesure où le porteur peut difficilement constater qu’un fraudeur est en possession d’une carte lui étant destinée. Dans ce cas de figure, le fraudeur s’attache à exploiter des vulnérabilités dans les procédures d’envoi des cartes. |
| Carte altérée ou contrefaite | La falsification d’une carte de paiement consiste à modifier les données magnétiques, d’embossage[[2]](#footnote-2) ou de programmation d’une carte authentique. La contrefaçon d’une carte suppose, quant à elle, la création d’un support donnant l’illusion d’être une carte de paiement authentique et/ou susceptible de tromper un automate ou un terminal de paiement de commerçant. Dans les deux cas, le fraudeur s’attache à ce qu’une telle carte supporte les données nécessaires pour tromper le système d’acceptation. |
| Numéro de carte usurpé | Le numéro de carte d’un porteur est relevé à son insu ou créé par « moulinage[[3]](#footnote-3) » et utilisé en vente à distance. |
| Autres | Tout autre motif de fraude comme l’utilisation d’un numéro de carte (ou PAN : Personnal Account Number) cohérent mais non attribué à un porteur, puis utilisé en vente à distance, la modification par le fraudeur d’un ordre de paiement légitime, la manipulation du payeur ayant pour effet d’obtenir un paiement par carte etc. |

* **Règles spécifiques devant être appliquées pour les établissements émettant des cartes co-badgées (CB-MasterCard ou CB-Visa) et destinées à prévenir les doubles comptes ou les omissions :**
* **Par le GIE CB** : ne déclarer que les transactions frauduleuses traitées4 par le système « CB » (indépendamment du fait que la carte utilisée soit une carte « CB only » ou une carte co-badgée) ;
* **Par MasterCard et Visa** : ne déclarer que les transactions frauduleuses traitées[[4]](#footnote-4) par le système MasterCard ou le système Visa (indépendamment du fait que la carte utilisée soit une carte « MasterCard Only », « Visa only » ou une carte co-badgée).

**Section 5. - Ventilation de la fraude en vente à distance par secteur d’activité sur les transactions nationales (émetteur FR/accepteur FR)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | Transactions | | Fraude | | Taux de fraude (%) |
| volume (en unités) | valeur (en euros) | volume (en unités) | valeur (en euros) |
| Commerce généraliste et semi-généraliste | |  |  |  |  |  |
| Produits techniques et culturels (livre, dvd, informatique, hi-fi, photo, vidéo, électroménager…) | |  |  |  |  |  |
| Voyage, transport | |  |  |  |  |  |
| Téléphonie et communication | |  |  |  |  |  |
| Alimentation | |  |  |  |  |  |
| Equipement de la maison, ameublement, bricolage | |  |  |  |  |  |
| Assurance | |  |  |  |  |  |
| Santé, Beauté, Hygiène | |  |  |  |  |  |
| Services aux particuliers et aux professionnels | |  |  |  |  |  |
| Approvisionnement d’un compte, vente de particulier à particulier | |  |  |  |  |  |
| Jeux en ligne | |  |  |  |  |  |
| Divers | |  |  |  |  |  |
| Total | |  |  |  |  |  |
|  | **5.2 - Commentaires supplémentaires** | | | | | |
|  | | | | | | |

Cette collecte concerne uniquement la vente à distance et les paiements domestiques (émetteur et commerçants français).

Afin de clarifier la manière dont les commerçants doivent être classés, quelques exemples sont présentés ci-dessous.

|  |  |
| --- | --- |
| Commerçants généralistes et semi-généralistes | 3suisses.fr, amazon.fr, auchan.fr, cdiscount.com, laredoute.fr, m6boutique.com, mistergooddeal.com, quelle.fr, vente-privee.com, vertbaudet.fr |
| Produits techniques et culturels (livre, dvd, informatique, hi-fi, photo, électroménager…) | alapage.com, , darty.com, fnac.com, franceloisirs.com, ldlc.com, pixmania.com, rueducommerce.fr, topachat.com |
| Voyage, transport | accorhotels.com, airfrance.fr, anyway.com, avis.fr, expedia.fr, nouvelles-frontieres.fr, opodo.fr, vivacances.fr, voyagesloisirs.com, voyages-sncf.com. |
| Téléphonie et communication | bouyguestelecom.fr, free.fr, orange.fr, sfr.fr |
| Alimentation | auchandirect.fr, houra.fr, ooshop.com, monoprix.com, telemarket.fr |
| Équipement de la maison, ameublement, bricolage | but.fr, castorama.fr, conforama.fr, ikea.fr, leroymerlin.fr |
| Assurance | europ-assistance.fr, mondial-assistance.fr |
| Santé, Beauté, Hygiène | ccbparis.fr, sephora.fr, yves-rocher.fr |
| Approvisionnement d’un compte, vente de particulier à particulier | ebay.fr, rakuten.com |
| Services aux particuliers et aux professionnels | store.apple.com, ticketnet.fr, ipsopresto.com, jm bruneau.fr, jpg.fr, ldlc pro.com, manutan.fr, officedepot.fr, raja.fr, vikingdirect.fr, welcomeoffice.com |
| Jeux en ligne | fdjeux.com, pmu.fr, betclic.fr |

Afin de faciliter le classement des commerçants dans ces catégories, vous pouvez vous référer à la liste des « Merchant Category Code » (MCC) suivante :



**5. Annexes**

**Glossaire**

|  |  |
| --- | --- |
|  | **> Accepteur** |
|  | Tout commerçant, tout prestataire de services et, d'une manière générale, toute personne morale ou physique de droit privé ou public recevant des fonds en paiement par carte, et ayant signé, à cette fin, un contrat d'acceptation avec sa banque ou avec l’organisme de gestion de cartes. |
|  | **> Acquéreur** |
|  | Établissement de crédit, institution ou service mentionné à l’article L. 518-1 du code monétaire et financier, lié à l’accepteur par un contrat et qui acquiert les données relatives aux transactions effectuées. L'acquéreur est notamment responsable de la collecte des transactions et du règlement des accepteurs, dans les limites des contrats en vigueur. |
|  | **> Carte contrefaite** |
|  | En automate : carte supportant les données nécessaires à tromper le système. |
|  | En commerce de proximité : carte fabriquée présentant peu ou prou le visuel, dont les sécurités, d’une carte authentique, supportant les données d’une carte d’un véritable porteur et destinée à tromper la vigilance d’un accepteur. |
|  | **> Carte de paiement** |
|  | La notion de carte de paiement est définie à l’article L. 132-1 du code monétaire et financier : |
|  | « Constitue une carte de paiement toute carte émise par un établissement de crédit ou par une institution ou un service mentionné à l’article L. 518-1 et permettant à son titulaire de retirer ou de transférer des fonds. » |
|  | **> Émetteur** |
|  | Organisme ou son agent qui a émis une carte de paiement au profit d’un porteur de carte et est lié à celui-ci par un contrat. |
|  | **> Numéro de carte usurpé** |
|  | Numéro de carte d’un porteur relevé à son insu ou créé par moulinage, et utilisé en vente à distance. |
|  |  |

**Zones géographiques**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Zone France**   |  | | --- | | France métropolitaine | | Départements et régions d’Outre-Mer[[5]](#footnote-5) : | | Guadeloupe | | Martinique | | Guyane française | | Réunion | | Saint Pierre et Miquelon | | Mayotte | | Saint Barthélemy | | Saint Martin | | Principauté de Monaco | | **Liste des pays de l’EEE (hors France)**   |  |  | | --- | --- | | Allemagne | (DE) | | Autriche | (AT) | | Belgique | (BE) | | Bulgarie | (BG) | | Chypre | (CY) | | Croatie | (HR) | | Danemark | (DK) | | Espagne | (ES) | | Estonie | (EE) | | Finlande | (FI) | | Grèce | (EL) | | Hongrie | (HU) | | Irlande | (IE) | | Islande | (IS) | | Italie | (IT) | | Lettonie | (LV) | | Liechtenstein | (LI) | | Lituanie | (LT) | | Luxembourg | (LU) | | Malte | (MT) | | Norvège | (NO) | | Pays-Bas | (NL) | | Pologne | (PL) | | Portugal | (PT) | | République tchèque | (CZ) | | Roumanie | (RO) | | Slovénie | (SI) | | Slovaquie | (SK) | | Suède | (SE) | |

1. Au sens autorisation et compensation. [↑](#footnote-ref-1)
2. Modification de l’impression en relief du numéro de carte. [↑](#footnote-ref-2)
3. Technique de fraude consistant à utiliser les règles, propres à un émetteur, de création de numéros de carte pour générer de tels numéros. [↑](#footnote-ref-3)
4. Au sens autorisation et compensation. [↑](#footnote-ref-4)
5. Les autres collectivités d’outre-mer (Polynésie française, Wallis et Futuna) et la Nouvelle-Calédonie, qui ne sont pas membres de l’Union européenne, ne font pas partie de la zone France. [↑](#footnote-ref-5)