Recensement de la fraude sur les moyens de paiement scripturaux

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

Collecte de l’Institut d’émission

d’outre-mer

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

**Guide de remplissage**

à l’attention des déclarants

**Applicable à partir des données 2023 collectées au S1 2024**



**Suivi des versions**

|  |  |  |
| --- | --- | --- |
| Version | Date | Commentaires |
| 1.0 | 08/12/2022 | Version initiale de l’IEOM |
| 1.1 | 01/12/2023 | Version post développements ONEGATE |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**SOMMAIRE**

[AVANT-PROPOS 1](#_Toc121414674)

[1. Introduction 1](#_Toc121414675)

[2. Établissements assujettis 2](#_Toc121414676)

[3. Présentation de la collecte 2](#_Toc121414677)

[3.1. Périmètre de la collecte 2](#_Toc121414678)

[3.1.1. Données collectées 2](#_Toc121414679)

[3.1.2. Ventilation des données collectées 3](#_Toc121414680)

[3.1.3. Données non concernées 5](#_Toc121414681)

[3.2. Évaluation de la fraude 5](#_Toc121414682)

[3.2.1. Définition de la fraude 6](#_Toc121414683)

[3.2.2. Typologie de la fraude 6](#_Toc121414684)

[3.2.3. Arbre de décision générique à tous les moyens de paiements sur le type de fraude 8](#_Toc121414685)

[3.3. Date de référence des données collectées 8](#_Toc121414686)

[3.4. Présentation des données collectées 8](#_Toc121414687)

[3.5. Modalités de déclaration 9](#_Toc121414688)

[4. Structure et contenu du questionnaire 10](#_Toc121414689)

[4.1. CARTES 10](#_Toc121414690)

[4.1.1. Fraude brute sur opérations par carte bancaire acquises par l’établissement - vue acquereur (tableau de l’onglet « Fraude 1.1 ») 11](#_Toc121414691)

[4.1.2. Fraude brute sur opérations effectuées par carte bancaire émise par l’établissement - vue émetteur (tableau de l’onglet « Fraude 1.2 ») 14](#_Toc121414692)

[4.1.3. Fraude sur opérations de retrait (tableaux de l’onglet « Fraude 1.3 ») 16](#_Toc121414693)

[4.1.4. Fraude sur retrait d’espèces sur DAB/GAB gérés par l’établissement (tableau de l’onglet « Fraude 1.3 ») 17](#_Toc121414694)

[4.2. VIREMENT 18](#_Toc121414695)

[4.2.1. Fraude brute sur les virements émis par l’établissement (tableau de l’onglet « Fraude 2.1 ») 18](#_Toc121414696)

[4.2.2. Virements faisant l’objet d’une demande de rappel de fonds (tableau de l’onglet « Fraude 2.2 ») 21](#_Toc121414697)

[4.3. CHEQUE 22](#_Toc121414698)

[4.3.1. Fraude brute sur les chèques reçus à l’encaissement par l’établissement (tableau de l’onglet « Fraude 3.1 ») 22](#_Toc121414699)

[4.3.2. Fraude brute portant sur les chèques de banque – établissement remettant (tableau de l’onglet « Fraude 3.2 ») 25](#_Toc121414700)

[4.4. PRELEVEMENT 25](#_Toc121414701)

[4.4.1. Fraude sur les prélèvements émis par l’établissement (tableau de l’onglet « Fraude 4.1 ») 25](#_Toc121414702)

[4.5. LETTRE DE CHANGE RELEVE (LCR) – BILLET À ORDRE (BOR) 28](#_Toc121414703)

[4.5.1. Fraude sur la Lettre de Change Relevé (LCR) et le Billet à Ordre relevé (BOR) (tableau de l’onglet « Fraude 5.1 ») 28](#_Toc121414704)

# AVANT-PROPOS

**Pourquoi un nouveau guide de remplissage ?**

Dans le cadre de la mission qui lui est confiée par l’article L. 721-24 du Code monétaire et financier, l’Institut d’émission d’outre-mer a fait le choix, dans le corpus réglementaire actuel encadrant les paiements, de modifier et enrichir le périmètre des collectes « Cartographie des moyens de paiement scripturaux » pour les données portant sur les transactions de paiement et « Recensement de la fraude sur les moyens de paiement scripturaux » pour les données relatives aux transactions frauduleuses.

**Quels sont les principaux changements ?**

* De nouveaux axes de répartition des données sont introduits : canal d’initiation, zone géographique et typologie de fraude ;
* Un suivi du recours à l’authentification forte et aux cas d’exemption ou d’exclusion à l’authentification forte est mis en place ;
* La déclaration prévoit un suivi du préjudice financier consécutif aux cas de fraude supporté par les établissements financiers et par les clients.

**À quelle date ce nouveau guide de remplissage s’applique ?**

En pratique, les prestataires de services de paiement (PSP) devront répondre à la collecte « Recensement de la fraude sur les moyens de paiement scripturaux », selon le format défini dans le présent guide de remplissage au titre des données de 2023 qui seront déclarées à l’Institut d’émission d’outre-mer au cours du premier semestre 2024.

# Introduction

Dans le cadre de sa mission de surveillance de la sécurité des moyens de paiement scripturaux (cf. article L. 721 - 24 du Code monétaire et financier), l’Institut d’émission d’outre-mer a mis en place un dispositif de collecte annuelle des données de fraude sur les moyens de paiement scripturaux.

Cette collecte couvre la fraude sur la carte de paiement, le virement, le chèque, le prélèvement et les effets de commerce (Lettre de Change Relevé et Billet à Ordre relevé) que les prestataires de service de paiement (PSP) mettent à la disposition de leur clientèle (particuliers, professionnels, entreprises, administrations).

Ces informations propres à chaque PSP sont collectées par l’IEOM sous couvert du secret professionnel défini à l’article L. 721-22 du Code monétaire et financer et ne sont pas destinées à être rendues publiques autrement que sous la forme agrégée de statistiques par collectivité.

Les résultats de cette collecte associés à ceux de la collecte « Cartographie des Moyens de Paiement Scripturaux » sont utilisés par l’IEOM pour calculer les taux de fraude du déclarant pour chacun des moyens de paiement scripturaux concernés. L’IEOM s’appuie également sur ces statistiques pour compléter sa veille technologique et sécuritaire.

Les informations collectées par l’Institut d’émission d’outre-mer à l’aide de ces deux questionnaires sont mises à la disposition du public dans un document publié sur son site Internet, uniquement sous forme agrégée et anonyme.

Le présent guide de remplissage a pour objet de fournir aux PSP toutes les informations nécessaires pour répondre à cette collecte.

# Établissements assujettis

Les PSP tenus de répondre à cette collecte sont :

* Les établissements de crédit, les établissements de paiement, les établissements de monnaie électronique et les prestataires de services d’information sur les comptes de droit français, agréés par l’Autorité de contrôle prudentiel et de résolution et dont le siège social est situé dans les Collectivités françaises du Pacifique ;
* Les émetteurs suivants : le Trésor public, les offices des postes et télécommunication, l'institut d'émission d'outre-mer et la Caisse des dépôts et consignations.

# Présentation de la collecte

## Périmètre de la collecte

### 3.1.1. Données collectées

Les données à déclarer portent sur le nombre et le montant des transactions frauduleuses effectuées par carte, par virement, par prélèvement, par chèque et par effet de commerce.

Les transactions frauduleuses à retenir sont celles qui résultent d’un **usage illicite du moyen de paiement ayant échappé au contrôle de l’un des deux établissements** (établissement du débiteur ou celui du créancier) **et ayant donné lieu à une écriture au compte du ou des clients après l’exécution de l’opération.**

Les données concernant les transactions frauduleuses doivent porter sur l’ensemble des transactions, quelles que soient les modalités d’échange (système d’échange interbancaire ou hors système, i.e. en intra-bancaire, en intra-groupe ou en bilatéral).

L**e montant de la fraude à déclarer doit correspondre au montant nominal du paiement (approche « fraude brute »)** sans prendre en compte l’impact des mesures prises dans le cadre des procédures contentieuses (par exemple, interruption de la livraison des produits ou de la fourniture de services, accord amiable pour le rééchelonnement du paiement en cas de répudiation abusive du paiement, dommages et intérêts suite à recours en justice, etc.).

La fraude comprend la fraude externe mais aussi la fraude interne, c'est-à-dire celle commise par un employé de l’établissement.

### 3.1.2. Ventilation des données collectées

Les transactions frauduleuses sont à ventiler selon plusieurs paramètres propres à chaque moyen/service de paiement : les types de fraude, les canaux d’initiation/d’autorisation de paiement, les zones géographiques, les méthodes d’authentification du client et le cas échéant les motifs d’exemption à l’authentification forte. Il est également demandé de déclarer la perte financière supportée consécutive à des transactions frauduleuses.

3.1.2.1. Précisions concernant certaines ventilations

**Qualification géographique des transactions :**

Afin de disposer d’une vue globale sur le Pacifique, ainsi que par collectivité, les transactions doivent être ventilées en :

* Transactions locales (intra-Collectivité) ;
* Transactions avec une autre Collectivité ;
* Transactions avec l’Hexagone et les DOM -la France- ;
* Transactions avec l’étranger.

**Méthode d’authentification du client :**

Les transactions frauduleuses doivent être ventilées selon le mode d’authentification utilisé par l’établissement : dispositifs d’authentification conformes ou non à l’arrêté du 14 janvier 2019.

|  |  |
| --- | --- |
| **Avec authentification forte du client** | Authentification du payeur reposant sur l’utilisation de deux éléments d'authentification sécurisés ou plus appartenant à au moins deux catégories différentes parmi la « connaissance » (quelque chose que seul l’utilisateur connaît), la « possession » (quelque chose que seul l’utilisateur possède) et l’« inhérence » (quelque chose que l’utilisateur est) et indépendants, en ce sens que la compromission de l’un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d’authentification. |
| **Sans authentification forte du client** | Authentification non conforme à la définition de l'authentification forte au sens de l’arrêté du 14/01/2019 :- utilisation d’un seul élément d'authentification sécurisé appartenant à l'une des catégories, parmi la « connaissance » (quelque chose que seul l’utilisateur connaît), la « possession » (quelque chose que seul l’utilisateur possède) et « l’inhérence » (quelque chose que l’utilisateur est) ;- ou, aucune utilisation d’élément d’authentification sécurisé. |

**Motifs d’exemption et d’exclusion à l’authentification forte du client :**

Les transactions frauduleuses n’ayant pas fait l’objet d’une authentification forte du client au sens de l’arrêté du 14/01/2019 (Cf. supra) doivent être ventilées selon le motif d’exemption auquel l’établissement a eu recours ou selon le motif d’exclusion pour les transactions n’entrant pas dans le périmètre de l’arrêté précité.

Pour ce qui concerne les transactions par carte, la ventilation par motif d’exemption est effectuée indépendamment du fait que ce soit l’émetteur ou l’acquéreur qui a déclenché le recours à l’exemption.

|  |  |
| --- | --- |
| **Article 11 Arrêté du 14/01/2019** | Paiement initié en proximité en mode sans contact d’un montant inférieur à 6 000 francs CFP dans la limite de 5 opérations successives ou 18 000 francs CFP de paiement cumulé. |
| **Article 12 Arrêté du 14/01/2019** | Paiement aux automates de transport et de parking. |
| **Article 13 Arrêté du 14/01/2019** | Paiement vers un bénéficiaire de confiance désigné préalablement comme tel par le payeur auprès de l’établissement teneur de compte.Pour les paiements par carte, l’émetteur déclare dans la rubrique « Dont au titre de l’art. 13 » et l’acquéreur dans la rubrique « Autres ». |
| **Article 14 Arrêté du 14/01/2019** | Série de paiements de même montant et vers le même bénéficiaire initiée par le payeur. Seule l’initiation de la première opération de paiement est soumise à l’authentification forte et doit être déclarée comme telle dans la présente collecte. |
| **Article 15 Arrêté du 14/01/2019** | Paiement entre les comptes tenus par l’établissement et détenus par la même personne physique ou morale. |
| **Article 16 Arrêté du 14/01/2019** | Paiement sur internet d’un montant inférieur à 3 600 francs CFP, dans la limite de 5 opérations successives ou de 12 000 francs CFP de paiement cumulé. |
| **Article 17 Arrêté du 14/01/2019** | Paiement recourant à des protocoles de transfert d’ordres de paiement sécurisés à destination des professionnels/entreprises pour lesquels les autorités compétentes ont acquis la certitude que lesdits procédures et protocoles garantissent des niveaux de sécurité au moins équivalents à ceux prévus par le [code monétaire et financier](https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026&dateTexte=&categorieLien=cid) |
| **Article 18 Arrêté du 14/01/2019** | Paiement électronique à distance présentant un faible niveau de risque au regard du dispositif de détection des opérations de paiement suspectes de l’établissement teneur de comptes. |
| **Paiements initiés par les commerçants (hors périmètre DPS2)** | Paiement initiés par le bénéficiaire sur la base d’un accord préexistant avec le payeur et le bénéficiaire pour les effectuer et donc non soumis à l’obligation de l’authentification forte du client (Cf. exigences fixées par la Commission européenne dans les Q&A 2018\_4131 et Q&A\_2018\_4031). |
| **Autres motifs d’exclusion (hors périmètre DSP2)** | Paiement dit « *One Leg* » c’est-à-dire lorsque le PSP du payeur ou celui du bénéficiaire est situé hors UE. |

**Pertes financières :**

Les pertes financières résultant d’une fraude correspondent au préjudice subi par l’établissement, son client et éventuellement d’autres parties prenantes de la transaction. Elles sont déterminées sur la base du montant brut de la fraude, déduction faite des fonds qui ont pu être recouvrés après les recours contentieux, mais elles ne doivent pas tenir compte des remboursements effectués par les organismes d’assurance.

Les pertes financières doivent être déclarées sur l’exercice au cours duquel elles ont été enregistrées comptablement, indépendamment de la date d’exécution de l’opération frauduleuse correspondante.

### 3.1.3. Données non concernées

Cette collecte ne concerne pas :

* Les transactions irrégulières du seul fait d’un **défaut de provision** suffisante.
* Lorsqu’un détournement de fonds résulte de l’usage d’un moyen de paiement par le personnel d’une entreprise cliente d’un établissement, et que ce personnel a **fait usage des droits qui lui sont accordés par son employeur et qui sont déclarés à l’établissement**, il ne doit pas être pris en compte dans ce questionnaire.
* Les **actes malveillants préparatoires** à l’utilisation frauduleuse d’un moyen de paiement mais ne constituant pas des attaques sur le moyen de paiement lui-même sont également exclus du périmètre du questionnaire :
* Les situations où le titulaire légitime du moyen de paiement effectue un paiement mais s’oppose au règlement, en détournant les procédures prévues par la loi, ou bien effectue un paiement en connaissance de cause sans disposer de la provision suffisante sont également hors périmètre ;
* Les actions visant à la récupération par le fraudeur de données personnelles en vue de leur utilisation ultérieure à des fins frauduleuses ne sont pas prises en compte (exemples : piratage de base de données, attaques de type « *phishing* » permettant de collecter sur Internet des données personnelles ou confidentielles, vol d’un chèque). Seuls les paiements réalisés ultérieurement, à l’aide des données frauduleusement collectées, sont inclus dans le périmètre de la collecte.

## Évaluation de la fraude

### Définition de la fraude

La fraude est définie comme l’utilisation illégitime d’un moyen 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 et/ou émetteur du moyen de paiement, le titulaire du moyen de paiement, le bénéficiaire légitime des fonds (l’accepteur et/ou créancier), 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 du moyen de paiement (vol, détournement du support du moyen de paiement ou des données qui lui sont attachées, piratage d’un équipement d’acceptation…) ;
	+ les modalités d’utilisation du moyen de paiement ou des données qui lui sont attachées (paiement/retrait en situation de proximité ou à distance, par utilisation physique de l’instrument de paiement ou des données qui lui sont attachées,…) ;
	+ la zone géographique d’émission ou d’utilisation du moyen de paiement ou des données qui lui sont attachées ;
* **et quelle que soit l’identité du fraudeur :** un tiers, l’établissement teneur de compte et/ou émetteur du moyen de paiement, le titulaire légitime du moyen de paiement, le bénéficiaire légitime des fonds, un tiers de confiance, etc.

### Typologie de la fraude

Les agissements frauduleux visés par la définition ci-dessus ont été classés selon une typologie harmonisée sur laquelle reposent les tableaux de déclaration.

1. Le fraudeur établit un **faux ordre** de paiement ;
	1. Au cas où l’usage d’un support matériel de paiement est exigé, il peut :
		1. Utiliser à la place de son titulaire légitime un moyen de paiement régulièrement émis, qu’il a obtenu après **perte, vol**, ou interception lors de son envoi ;
		2. Utiliser un moyen de paiement **altéré ou contrefait**. Les données d’identification qu’il utilise sont totalement ou partiellement fictives.
	2. Il peut, sinon, utiliser des données bancaires fictives ou appartenant à un tiers, lorsqu’elles sont suffisantes pour effectuer le paiement (numéro de compte, login / mot de passe, …).
2. Le fraudeur **détourne et/ou falsifie** un ordre de paiement régulièrement émis par le titulaire légitime du moyen de paiement, ce qui couvre :
	1. La simple **utilisation ou la réutilisation** d’un ordre de paiement régulier ;
	2. La **modification d’un des attributs** (montant, nom du bénéficiaire ou du donneur d’ordre…) d’un ordre de paiement régulier.
3. Le fraudeur ouvre un compte sous une fausse identité, grâce à laquelle il obtient un moyen de paiement et réalise des ordres de paiement. La fraude est constituée lorsque le fraudeur disparait en laissant un compte à découvert ou une ligne de crédit.

Remarques :

* Dès lors qu’il y a modification d’un des attributs d’un ordre de paiement régulièrement émis, il faut considérer la fraude comme une falsification et non un détournement.
* Le détournement ne s’applique que lorsque le moyen de paiement, par exemple un chèque, fait l’objet d’une utilisation/réutilisation simple sans modification d’attribut (e.g. le fraudeur encaisse le chèque non altéré sur un compte qui n’est pas détenu par le bénéficiaire légitime).
* Le détournement intègre les opérations de paiement effectuées à la suite d’une manipulation du payeur par le fraudeur, ayant pour effet d’émettre un ordre de paiement ou de donner instruction de le faire vers un compte de paiement que le payeur estime appartenir à un bénéficiaire légitime, **dès lors que le fraudeur intervient directement ou indirectement dans le processus de paiement**. Sont donc à considérer comme répondant à cette définition et devant être déclarés les cas de :
	+ Fraude au président ;
	+ Fraude au changement de coordonnées bancaires ;
	+ Fraude au faux technicien bancaire ou faux test informatique ;
	+ Fraude par attaque de *phishing* seulement si celle-ci conduit le payeur à exécuter une opération de paiement. En revanche, si l’attaque par *phishing* permet au fraudeur de récupérer des données de paiement du payeur puis de les utiliser ensuite pour réaliser lui-même une opération de paiement, la fraude est à déclarer dans la typologie « Faux ».

 Cette liste ne saurait être exhaustive.

En revanche, sont à exclure :

* + Les cas d’escroqueries où le payeur effectue un paiement vers un bénéficiaire qui est un fraudeur, dans la mesure où le produit ou le service acheté n’existe pas et n’est donc pas livré (par exemple, cas de faux site internet de vente de produits financiers) ;
	+ Les cas de litiges commerciaux (par exemple, cas d’un site en faillite qui ne livre pas les produits commandés ou lorsque l’objet acheté ou le service rendu n’est pas conforme à la commande) ;

Lorsque l’établissement est confronté à une situation dans laquelle la fraude s’apparente à plusieurs types de fraude tels que définis dans la typologie ci-dessus, il se reportera, pour sa déclaration, au type de fraude qui lui semble caractériser de façon prédominante la situation rencontrée.

### Arbre de décision générique à tous les moyens de paiements sur le type de fraude

Cet arbre de décision constitue une aide à la classification de la fraude. Il est décliné pour chacun des moyens de paiement dans la suite du document. Les établissements qui le souhaitent, pourront s’y référer en cas de doute sur la classification de certains cas de fraude rencontrés.

|  |
| --- |
|  |

## Date de référence des données collectées

La date de référence pour la déclaration de la fraude est la **date d’exécution de l’opération frauduleuse** et non la date à laquelle la fraude a été découverte et/ou déclarée.

## Présentation des données collectées

Les données en volume (nombre de transactions) doivent être déclarées en unités et celles exprimées en valeur (montant des transactions) en francs CFP sans décimales.

Si les données sources sont dans une autre devise, il convient de les convertir en euros en utilisant de préférence les taux de change de référence moyen publiés par la BCE ([www.ecb.int](http://www.ecb.int), *Euro foreign exchange reference rates*), sauf si l’établissement déclarant a retenu une autre méthode (par exemple, conversion au jour le jour).

Lorsqu’un établissement n’a pas recensé de fraude durant l’exercice sous revue, il lui est demandé de renseigner la ou les rubrique(s) à zéro (« 0 »).

Des règles de contrôle à appliquer par les établissements sont paramétrées dans le questionnaire afin d’assurer la cohérence et l’exhaustivité des données déclarées.

**Les établissements sont invités à contrôler avec la plus grande rigueur la fiabilité des données qu’ils déclarent.** En effet, une déclaration erronée peut avoir des conséquences très dommageables sur la qualité des statistiques utilisées pour la surveillance des moyens de paiement exercée par l’IEOM.

## Modalités de déclaration

La déclaration est établie sur une base annuelle. Les périodes de collecte s’étendent pour l’enregistrement des données du 1er jour ouvrable de février au dernier jour ouvrable de mars de l’année N pour les données de l’exercice N-1.

Les établissements déclarants sont informés des périodes de collecte chaque année par l’Institut d’émission d’outre-mer.

La déclaration s’effectue au travers du portail ONEGATE – OSCAMPS (portail de déclaration de la Banque de France) dont les modalités d’accès sont précisées dans le manuel utilisateur externe ONEGATE disponible sur le site internet de la Banque de France (www.banque-france.fr, rubrique OSCAMPS).

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

**Pour toute information, vous pouvez contacter les services de la Banque de France et de l’Institut d’émission d’outre-mer à partir des coordonnées suivantes :**

|  |  |
| --- | --- |
| Support-ONEGATE@banque-france.fr | Pour les questions relatives au portail de déclaration ONEGATE. |
| IEOM-Paris-SEF-surveillance@iedom-ieom.fr | Pour les questions relatives au contrat d'interface remettant. |
| L’agence IEOM de votre Collectivité (PMSB@ieom.nc ; IEOM-WF-Comptabilite@ieom.wf ; PMSB@ieom.pf) ou les services du siège (IEOM-Paris-SEF-surveillance@iedom-ieom.fr) | Pour les questions portant sur la gestion opérationnelle de la collecte.  |
| IEOM-Paris-SEF-surveillance@iedom-ieom.fr | Pour les questions d'ordre méthodologique pour lesquelles le présent guide de remplissage n'apporte pas de réponse. |

# Structure et contenu du questionnaire

Les chapitres suivants renvoient aux onglets du fichier Excel de présentation des tableaux de collecte des données :



## CARTES

Il s’agit de déclarer, en nombre et en valeur, les opérations de paiement et de retrait frauduleuses effectuées par cartes de paiement et dont les paiements sont acquis par les clients de l’établissement. Une ventilation par typologie de fraude, canal d’initiation, zone géographique, méthode d’authentification et motif de dérogation à l’authentification forte est attendue.

Remarques :

* Sont concernées toutes les cartes, quelle que soit leur catégorie (carte de débit, carte de crédit ou carte de débit différé, carte commerciale) et quel que soit le réseau d’acceptation (interbancaire ou privatif).
* Sont exclues les cartes dotées uniquement d’une fonction de monnaie électronique (par exemple, les cartes prépayées) qui sont à déclarer dans la fonction « Monnaie électronique ».
* Si l’établissement acquéreur n’est pas en mesure de ventiler les opérations de paiement et de retrait frauduleuses, il peut fournir des données estimées en précisant, dans ce cas, la méthode d’estimation qu’il a utilisée en commentaires.
* **Typologie de fraude :**

|  |  |  |
| --- | --- | --- |
| Faux | 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 de la carte. |
| 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 contrefaite | Le fraudeur utilise (i) une carte contrefaite, qui suppose 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 ou (ii) d’une carte falsifiée qui consiste à modifier les données magnétiques, d’embossage ou de programmation d’une carte authentique. 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 usurpée | Le numéro de carte d’un porteur est relevé à son insu ou créé par « moulinage » et utilisé en vente à distance. |
| Autres cas | Par exemple, utilisation d’un numéro de carte (ou PAN : personnal account number) cohérent mais non attribué à un porteur, puis généralement utilisé en vente à distance. |
| Falsification  | Ordre de paiement par carte initié par le porteur légitime qui est ensuite modifié par un fraudeur. |
| Détournement | Paiement ou retrait sous la contrainte.  |

* **Canal d’initiation :**

|  |  |
| --- | --- |
| Non électronique | Paiement initié par un canal de type : courrier, formulaire, courriel, télécopie ou téléphone. Ces canaux ont en commun de nécessiter la re-saisie des instructions de paiement du payeur. |
| Voie électronique | À distance sur internet + proximité.  |
| À distance sur internet | Paiement initié depuis un canal internet, à partir d’un ordinateur, d’un téléphone portable ou d’un dispositif similaire. |
| Proximité  | Paiement initié depuis un terminal physique (point de vente ou sur automate), y compris en mode sans contact. |

* **Zone géographique :**

|  |  |  |
| --- | --- | --- |
| Moyen de paiement | Déclarant | Localisation contrepartie |
| Carte de paiement | Vue acquéreur | Localisation par zone géographique du PSP émetteur de la carte de paiement (COM, Autres COM, France et Etranger) |
| Vue émetteur | Localisation par zone géographique de réalisation de la transaction (COM, Autres COM, France et Etranger) |

### Fraude brute sur opérations par carte bancaire acquises par l’établissement - vue acquereur (tableau ONEGATE, écran « 1.1 – Fraude brute sur opérations par carte bancaire acquises par l’établissement (vue acquéreur) »)

* **Données à déclarer :**

|  |  |
| --- | --- |
|  | Par zone géographique d’émission des cartes de paiement (COM, Autres COM, France et Etranger) |
|  | Volume en unités | Valeur enF CFP |
| (1) Fraude brute sur opérations par cartes acquises par l’établissement (vue acquéreur) |  |  |
|  | **(2) Dont paiements initiés par voie non électronique (MOTO) –A distance et en proximité-** |  |  |
|  | **(3) Dont paiements initiés par voie électronique** |  |  |
|  |  | **(4) Dont paiements initiés à distance** |  |  |
|  |  |  | **(5) Dont avec authentification forte du client** |  |  |
|  |  |  |  | *(6) Dont Faux* |  |  |
|  |  |  |  |  | *(7) Dont avec carte perdue / volée* |  |  |
|  |  |  |  |  | *(8) Dont avec carte non reçue* |  |  |
|  |  |  |  |  | *(9) Dont avec carte contrefaite* |  |  |
|  |  |  |  |  | *(10) Dont avec numéro de carte usurpé* |  |  |
|  |  |  |  |  | *(11) Dont autres cas* |  |  |
|  |  |  |  | *(12) Dont Falsification* |  |  |
|  |  |  |  | *(13)Dont Détournement* |  |  |
|  |  |  | **(14) Dont sans authentification forte du client** |  |  |
|  |  |  |  | *(15) Dont Faux* |  |  |
|  |  |  |  |  | *(16) Dont avec carte perdue / volée* |  |  |
|  |  |  |  |  | *(17) Dont avec carte non reçue* |  |  |
|  |  |  |  |  | *(18) Dont avec carte contrefaite* |  |  |
|  |  |  |  |  | *(19) Dont avec numéro de carte usurpé* |  |  |
|  |  |  |  |  | *(20) Dont autres cas* |  |  |
|  |  |  |  | *(21) Dont Falsification* |  |  |
|  |  |  |  | *(22) Dont Détournement* |  |  |
|  |  |  |  | *(23) Dont au titre de l’Art. 14 de l’arrêté (opération récurrente)* |  |  |
|  |  |  |  | *(24) Dont au titre de l’Art. 16 de l’arrêté (Faible montant)* |  |  |
|  |  |  |  | *(25) Dont au titre de l’Art. 18 de l’arrêté (Analyse des risques)* |  |  |
|  |  |  |  | *(26) Dont au titre des paiements initiés par les commerçants* |  |  |
|  |  |  |  | *(27) Dont au titre d’autres motifs d’exclusion* |  |  |
|  |  | **(28) Dont paiements initiés en proximité** |  |  |
|  |  |  | **(29) Dont avec authentification forte du client** |  |  |
|  |  |  |  | *(30) Dont Faux* |  |  |
|  |  |  |  |  | *(31) Dont avec carte perdue / volée* |  |  |
|  |  |  |  |  | *(32) Dont avec carte non reçue* |  |  |
|  |  |  |  |  | *(33) Dont avec carte contrefaite* |  |  |
|  |  |  |  |  | *(34) Dont avec numéro de carte usurpé* |  |  |
|  |  |  |  |  | *(35) Dont autres cas* |  |  |
|  |  |  |  | *(36) Dont Falsification* |  |  |
|  |  |  |  | *(37) Dont Détournement* |  |  |
|  |  |  | **(38) Dont sans authentification forte du client** |  |  |
|  |  |  |  | *(39) Dont Faux* |  |  |
|  |  |  |  |  | *(40) Dont avec carte perdue / volée* |  |  |
|  |  |  |  |  | *(41) Dont avec carte non reçue* |  |  |
|  |  |  |  |  | *(42) Dont avec carte contrefaite* |  |  |
|  |  |  |  |  | *(43) Dont avec numéro de carte usurpé* |  |  |
|  |  |  |  |  | *(44) Dont autres cas* |  |  |
|  |  |  |  | *(45) Dont Falsification* |  |  |
|  |  |  |  | *(46) Dont Détournement* |  |  |
|  |  |  |  | *(47) Dont au titre de l’Art. 11 de l’arrêté (Paiement sans contact de faible montant)* |  |  |
|  |  |  |  | *(48) Dont au titre de l’Art. 12 de l’arrêté (Automates transport / parking)* |  |  |
|  |  |  |  | *(49) Dont au titre de l’Art. 14 de l’arrêté (opération récurrente)* |  |  |
|  |  |  |  | *(50) Dont au titre d’autres motifs d’exclusion* |  |  |

|  |  |  |
| --- | --- | --- |
|  |  | Total Valeur |
| (51) Pertes financières supportées par l’établissement déclarant |  |  |
| (52) Pertes financières supportées par l’utilisateur du service de paiement (bénéficiaire du paiement) |  |  |

* **Contrôles :**

Les règles de contrôle suivantes doivent être appliquées :

|  |
| --- |
| En volume et en valeur et dans les différentes rubriques, le total de chaque indicateur est = à la somme des quatre sous-ventilations géographiques associées (Cartes émises dans la COM du déclarant + Cartes émises dans une autre COM + Cartes émises en Métropole et DOM + Cartes émises à l’étranger).Cette règle ne s’applique pas aux opérations fraudées réalisées sans identification forte du client, sur la base d’une exemption ou d’autres motifs d’exclusion listés dans l’arrêté du 14 janvier 2019. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur opérations par carte bancaire acquises par l’établissement (vue acquéreur) est = à la somme de la fraude brute sur paiement initié par voie non électronique (MOTO) – A distance et en proximité- et de la fraude brute sur paiement initié par voie électronique. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude sur les paiements initiés par voie électronique est = à la somme de la fraude sur les paiements initiés à distance et de la fraude sur les paiements initiés en proximité. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude sur les paiements initiés à distance est = à la somme de la fraude sur les paiements initiés à distance avec authentification forte du client et de la fraude sur les paiements initiés à distance sans authentification forte du client. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés à distance avec une authentification forte du client sont = à la somme des paiements fraudés de type faux, de type falsification et de type détournement.  |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés à distance sans authentification forte du client sont = à la somme des paiements fraudés de type faux, de type falsification et de type détournement. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés à distance avec ou sans authentification forte du client et de type faux sont = à la somme des paiements fraudés réalisés par utilisation de cartes perdues / volées, de cartes non reçues, de cartes contrefaites, de numéro de carte usurpé et d’autres cas . |
| En volume et en valeur, uniquement en Total, les paiements fraudés initiés à distance sans authentification forte du client sont = à la somme des paiements fraudés après usage des exemptions de l’article 14, de l’article 16, de l’article 18 de l’arrêté du 14/01/2019, des paiements initiés par les commerçants et des paiements relevant d’un autre motif d’exclusion. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés en proximité sont = à la somme des paiements fraudés initiés en proximité avec authentification forte du client et des paiements fraudés initiés en proximité sans authentification forte du client. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés en proximité avec une authentification forte du client sont = à la somme des paiements fraudés de type faux, de type falsification et de type détournement.  |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés en proximité sans authentification forte du client sont = à la somme des paiements fraudés de type faux, de type falsification et de type détournement. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés en proximité avec ou sans authentification forte du client et de type faux sont = à la somme des paiements fraudés réalisés par utilisation de cartes perdues / volées, de cartes non reçues, de cartes contrefaites, de numéro de carte usurpé et d’autres cas . |
| En volume et en valeur, et uniquement en Total, les paiements fraudés initiés en proximité sans authentification forte du client sont = à la somme des paiements fraudés après usage des exemptions de l’article 11, de l’article 12, de l’article 14 de l’arrêté et des paiements relevant d’un autre motif d’exclusion. |

### Fraude brute sur opérations effectuées par carte bancaire émise par l’établissement - vue émetteur (ONEGATE, écran « 1.2 – Fraude brute sur opérations effectuées par cartes bancaires émises par l’établissement (vue émetteur) »)

* **Données à déclarer :**

|  |  |
| --- | --- |
|  | Par zone géographique de réalisation de la transaction (COM, Autres COM, France et Etranger) |
|  | Volume en unités | Valeur enF CFP |
| (1) Fraude brute sur opérations effectuées par cartes émises par l’établissement (vue émetteur) |  |  |
|  | **(2) Dont paiements initiés par voie non électronique (MOTO) –A distance et en proximité-** |  |  |
|  | **(3) Dont paiements initiés par voie électronique** |  |  |
|  |  | **(4) Dont paiements initiés à distance** |  |  |
|  |  |  | **(5) Dont avec authentification forte du client** |  |  |
|  |  |  |  | *(6) Dont Faux* |  |  |
|  |  |  |  |  | *(7) Dont avec carte perdue / volée* |  |  |
|  |  |  |  |  | *(8) Dont avec carte non reçue* |  |  |
|  |  |  |  |  | *(9) Dont avec carte contrefaite* |  |  |
|  |  |  |  |  | *(10) Dont avec numéro de carte usurpé* |  |  |
|  |  |  |  |  | *(11) Dont autres cas* |  |  |
|  |  |  |  | *(12) Dont Falsification* |  |  |
|  |  |  |  | *(13) Dont Détournement* |  |  |
|  |  |  | **(14) Dont sans authentification forte du client** |  |  |
|  |  |  |  | *(15) Dont Faux* |  |  |
|  |  |  |  |  | *(16) Dont avec carte perdue / volée* |  |  |
|  |  |  |  |  | *(17) Dont avec carte non reçue* |  |  |
|  |  |  |  |  | *(18) Dont avec carte contrefaite* |  |  |
|  |  |  |  |  | *(19) Dont avec numéro de carte usurpé* |  |  |
|  |  |  |  |  | *(20) Dont autres cas* |  |  |
|  |  |  |  | *(21) Dont Falsification* |  |  |
|  |  |  |  | *(22) Dont Détournement* |  |  |
|  |  |  |  | *(23) Dont au titre de l’Art. 13 de l’arrêté (Bénéficiaire de confiance)* |  |  |
|  |  |  |  | *(24) Dont au titre de l’Art. 14 de l’arrêté (Opération récurrente)* |  |  |
|  |  |  |  | *(25) Dont au titre de l’Art. 16 de l’arrêté (Faible montant)* |  |  |
|  |  |  |  | *(26) Dont au titre de l’Art. 17 de l’arrêté (Protocole de paiement sécurisé)* |  |  |
|  |  |  |  | *(27) Dont au titre de l’Art. 18 de l’arrêté (Analyse des risques)* |  |  |
|  |  |  |  | *(28) Dont au titre des paiements initiés par les commerçants* |  |  |
|  |  |  |  | *(29) Dont au titre d’autres motifs d’exclusion* |  |  |
|  |  | **(30) Dont paiements initiés en proximité** |  |  |
|  |  |  | **(31) Dont avec authentification forte du client** |  |  |
|  |  |  |  | *(32) Dont Faux* |  |  |
|  |  |  |  |  | *(33) Dont avec carte perdue / volée* |  |  |
|  |  |  |  |  | *(34) Dont avec carte non reçue* |  |  |
|  |  |  |  |  | *(35) Dont avec carte contrefaite* |  |  |
|  |  |  |  |  | *(36) Dont avec numéro de carte usurpé* |  |  |
|  |  |  |  |  | *(37) Dont autres cas* |  |  |
|  |  |  |  | *(38) Dont Falsification* |  |  |
|  |  |  |  | *(39) Dont Détournement* |  |  |
|  |  |  | **(40) Dont sans authentification forte du client** |  |  |
|  |  |  |  | *(41) Dont Faux* |  |  |
|  |  |  |  |  | *(42) Dont avec carte perdue / volée* |  |  |
|  |  |  |  |  | *(43) Dont avec carte non reçue* |  |  |
|  |  |  |  |  | *(44) Dont avec carte contrefaite* |  |  |
|  |  |  |  |  | *(45) Dont avec numéro de carte usurpé* |  |  |
|  |  |  |  |  | *(46) Dont autres cas* |  |  |
|  |  |  |  | *(47) Dont Falsification* |  |  |
|  |  |  |  | *(48) Dont Détournement* |  |  |
|  |  |  |  | *(49) Dont au titre de l’Art. 11 de l’arrêté (Paiement sans contact de faible montant)* |  |  |
|  |  |  |  | *(50) Dont au titre de l’Art. 12 de l’arrêté (Automates transport / parking)* |  |  |
|  |  |  |  | *(51) Dont au titre de l’Art. 13 de l’arrêté Bénéficiaire de confiance)* |  |  |
|  |  |  |  | *(52) Dont au titre de l’Art. 14 de l’arrêté (opération récurrente)* |  |  |
|  |  |  |  | *(53) Dont au titre d’autres motifs d’exclusion* |  |  |

|  |  |  |
| --- | --- | --- |
|  |  | Total Valeur |
| (54) Pertes financières supportées par l’établissement déclarant |  |  |
| (55) Pertes financières supportées par l’utilisateur du service de paiement (bénéficiaire du paiement) |  |  |

* **Contrôles :**

Les règles de contrôle suivantes doivent être appliquées :

|  |
| --- |
| En volume et en valeur, sur les différentes rubriques, le total de chaque indicateur est = à la somme des quatre sous-ventilations géographiques associées (Transactions effectuées dans la COM du déclarant + transactions effectuées dans une autre COM + Transaction effectuées en Métropole ou DOM + Transactions effectuées à l’étranger).Cette règle ne s’applique pas aux opérations fraudées réalisées sans identification forte du client sur la base d’une exemption listée dans l’arrêté du 14 janvier 2019. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur les opérations effectuées par cartes émises par l’établissement (vue émetteur) est = à la somme de la fraude brute sur les paiement initiés par voie non électronique (MOTO) – A distance et en proximité- et de la fraude brute sur les paiement initiés par voie électronique. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude sur les paiements initiés par voie électronique est = à la somme de la fraude sur les paiement initiés à distance et de la fraude sur les paiements initiés en proximité. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude sur les paiements initiés à distance est = à la somme de la fraude sur les paiements initiés à distance avec authentification forte du client et de la fraude sur les paiements initiés à distance sans authentification forte du client. |
| En volume et en valeur en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés à distance avec une authentification forte du client sont = à la somme des paiements fraudés de type faux, de type falsification et de type détournement.  |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés à distance sans authentification forte du client sont = à la somme des paiements fraudés de type faux, de type falsification et de type détournement. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés à distance avec ou sans authentification forte du client et de type faux sont = à la somme des paiements fraudés réalisés par utilisation de cartes perdues / volées, de cartes non reçues, de cartes contrefaites, de numéros de cartes usurpés et d’autres cas . |
| En volume et en valeur, et uniquement en Total, les paiements fraudés initiés à distance sans authentification forte du client sont = à la somme des paiements fraudés après usage des exemptions de l’article 13, de l’article 14, de l’article 16, de l’article 17, de l’article 18 de l’arrêté, des paiements initiés par les commerçants et des paiements relevant d’un autre motif d’exclusion. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés en proximité sont = à la somme des paiements fraudés initiés en proximité avec authentification forte du client et des paiements fraudés initiés en proximité sans authentification forte du client. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés en proximité avec une authentification forte du client sont = à la somme des paiements fraudés de type faux, de type falsification et de type détournement.  |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés en proximité sans authentification forte du client sont = à la somme des paiements fraudés de type faux, de type falsification et de type détournement. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, les paiements fraudés initiés en proximité avec ou sans authentification forte du client et de type faux sont = à la somme des paiements fraudés réalisés par utilisation de cartes perdues / volées, de cartes non reçues, de cartes contrefaites, de numéro de carte usurpé et d’autres cas . |
| En volume et en valeur, et uniquement en Total, les paiements fraudés initiés en proximité sans authentification forte du client sont = à la somme des paiements fraudés après usage des exemptions de l’article 11, de l’article 12, de l’article 13, de l’article 14 de l’arrêté du 14/01/2019 et des paiements relevant d’un autre motif d’exclusion. |
|  |

### Fraude sur opérations de retrait (ONEGATE, écran « 1.3.A – Fraude brute sur retrait d’espèces sur DAB/GAB par cartes bancaires émises par votre établissement »)

* **Données à déclarer :**

|  |  |
| --- | --- |
|  | Par zone géographique de réalisation de la transaction (COM, Autres COM, France et Etranger) |
|  | Volume en unités | Valeur enF CFP |
| (1) Fraude brute sur retrait d’espèces sur DAB / GAB par cartes bancaires émises par votre établissement |  |  |
|  | (2) Dont Faux- |  |  |
|  |  | (3) Dont avec carte perdue / volée |  |  |
|  |  | (4) Dont avec carte non reçue |  |  |
|  |  | (5) Dont avec carte contrefaite |  |  |
|  |  | (6) Dont autres cas |  |  |
|  | (7) Dont Détournement |  |  |

* **Contrôles :**

Les règles de contrôle suivantes doivent être appliquées :

|  |
| --- |
| En volume et en valeur, le total de chaque indicateur est = à la somme des quatre sous-ventilations géographiques associées (Transactions effectuées dans la COM du déclarant + transactions effectuées dans une autre COM + Transaction effectuées en Métropole ou DOM + Transactions effectuées à l’étranger). |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur retrait d’espèces sur DAB / GAB par cartes émises par votre établissement est = à la somme de la fraude brute de type faux et de la fraude brute de type détournement. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur retrait d’espèces sur DAB / GAB par cartes émises par votre établissement de type Faux est = à la somme des retraits fraudés réalisés par utilisation de cartes perdues / volées, de cartes non reçues, de cartes contrefaites et d’autres cas de fraude. |

### Fraude sur retrait d’espèces sur DAB/GAB gérés par l’établissement (ONEGATE, écran « 1.3.B – Fraude brute sur retrait d’espèces sur DAB/GAB gérés par votre établissement »)

* **Données à déclarer :**

|  |  |
| --- | --- |
|  | Par zone géographique d’émission des cartes de paiement (COM, Autres COM, France et Etranger) |
|  | Volume en unités | Valeur enF CFP |
| (1) Fraude brute sur retrait d’espèces sur DAB / GAB gérés par l’établissement |  |  |
|  | (2) Dont Faux- |  |  |
|  |  | (3) Dont avec carte perdue / volée |  |  |
|  |  | (4) Dont avec carte non reçue |  |  |
|  |  | (5) Dont avec carte contrefaite |  |  |
|  |  | (6) Dont autres cas |  |  |
|  | (7) Dont Détournement |  |  |

* **Contrôles :**

Les règles de contrôle suivantes doivent être appliquées :

|  |
| --- |
| En volume et en valeur et dans les différentes rubriques, le total de chaque indicateur est = à la somme des quatre sous-ventilations géographiques associées (cartes émises dans la COM du déclarant + dans une autre COM + en Métropole ou DOM + cartes émises à l’étranger). |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur retrait d’espèces sur DAB / GAB gérés par l’établissement est = à la somme de la fraude brute de type faux et de la fraude brute de type détournement. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur retrait d’espèces sur DAB / GAB gérés par l’établissement de type Faux est = à la somme des retraits fraudés réalisés par utilisation de carte perdue / volée, de carte non reçue, de carte contrefaite et d’autres cas de fraude. |

## VIREMENT

###  Fraude brute sur les virements émis par l’établissement (ONEGATE, écran « 2.1 – Fraude brute sur virements émis par l’établissement »)

Il s’agit de déclarer, en nombre et en valeur, la fraude sur les virements émis par l’établissement en tant que PSP du payeur (ou du donneur d’ordre) avec une ventilation par typologie de fraude, canal d’initiation, zone géographique, méthode d’authentification et, le cas échéant, par motif de dérogation à l’authentification forte.

Remarques :

* Tous les types de virements sont concernés : virements locaux, virements SEPACOM, virements internationaux et virements instantanés ;
* Les transactions visées sont les virements de clientèle (particuliers, professionnels, entreprises, administrations…), quel que soit le mode d’échange utilisé pour la remise de l’ordre de virement. Sont exclus les virements entre IFM (Institutions Financières Monétaires) liés notamment au règlement d’opérations de marché, de trésorerie ou encore de compensation.
* **Typologie de fraude :**

|  |  |
| --- | --- |
| Faux | Le fraudeur contrefait un ordre de virement ou usurpe les identifiants de la banque en ligne du donneur d’ordre légitime afin d’initier un ordre de paiement. Dans ce cas de figure, les identifiants peuvent notamment être obtenus via des procédés de piratage informatique (phishing, malware, etc.) ou sous la contrainte. |
| Falsification  | Le fraudeur intercepte et modifie un ordre de virement ou un fichier de remise de virement légitime. |
| Détournement | Le fraudeur amène, par la tromperie (notamment de type ingénierie sociale, c’est-à-dire en usurpant l’identité d’un interlocuteur du payeur : responsable hiérarchique, fournisseur, technicien bancaire, etc.) ou par la contrainte, le titulaire légitime du compte à émettre régulièrement un virement à destination d’un numéro de compte qui n’est pas celui du bénéficiaire légitime du paiement ou qui ne correspond à aucune réalité économique. |

* **Arbre de décision sur le type de fraude au virement :**

Les établissements qui le souhaitent pourront se référer à l’arbre de décision ci-dessous en cas de doute sur la classification de certains cas de fraude relatifs au virement.

|  |
| --- |
|  |

* **Canal d’initiation :**

|  |  |
| --- | --- |
| Non électronique  | Ordre de virement transmis par un canal de type : courrier, formulaire, courriel, télécopie ou téléphone. Ces canaux ont en commun de nécessiter la re-saisie des instructions de paiement du payeur. |
| Électronique | Ordre de virement qui peut être transmis à distance ou en mode non distant. |
| À distance | Ordre de virement qui peut être transmis par Internet ou par voie télématique. |
| Internet | Ordre de virement transmis depuis la banque en ligne ou par une application de paiement mobile. |
| Télématique | Ordre de virement transmis via d’autres canaux électroniques hors banque en ligne et application de paiement mobile, tels que par exemple le système EBICS (electronic banking internet communication standard, canal de communication interbancaire permettant aux entreprises de réaliser des transferts de fichiers automatisés avec une banque. |
| Non distant | Ordre de virement initié au guichet bancaire ou depuis un GAB. |

* **zone géographique :**

|  |  |
| --- | --- |
| Virement local | Ordre de virement émis vers un PSP du bénéficiaire situé dans la collectivité du déclarant. |
| Virement vers une autre COM. | Ordre de virement émis vers un PSP du bénéficiaire situé dans une autre COM. |
| Virement vers la Métropole ou un DOM. | Ordre de virement émis vers un PSP du bénéficiaire situé en France métropolitaine ou dans un DOM. |
| Virement vers l’étranger. | Ordre de virement émis vers un PSP du bénéficiaire situé à l’étranger. |

* **type de virement :**

|  |  |
| --- | --- |
| Virement local   | Virement pour lequel le payeur et le bénéficiaire ont un compte ouvert dans des banques implantées dans la même Collectivité |
| Virement SEPACOM | Virement conforme aux exigences énoncées dans l’article L. 722-1 du Code monétaire et financier, le décret n° 2014-59 du 27 janvier 2014 et l’arrêté du 27 janvier 2014. |

* **Données à déclarer :**

|  |  |
| --- | --- |
|  | Par zone géographique de réalisation de la transaction (COM, Autres COM, France et Etranger) |
|  | Volume en unités | Valeur enF CFP |
| (1) Fraude brute sur virement émis par l’établissement |  |  |
|  | **(2) Dont virements non électroniques initiés sur support papier** |  |  |
|  | **(3) Dont virement non électronique initiés via un autre support** |  |  |
|  | **(4) Dont virements initiés par voie électronique** |  |  |
|  |  | (5) Dont virements initiés par lot / fichier |  |  |
|  |  | (6) Dont virements initiés depuis la banque en ligne |  |  |
|  |  | (7) Dont virements initiés depuis un GAB ou un autre terminal |  |  |
|  |  | (8) Dont virements initiés depuis une solution de paiement mobile |  |  |
|  |  | **(9) Dont avec authentification forte du client** |  |  |
|  |  |  | *(10) Dont Faux* |  |  |
|  |  |  | *(11) Dont Falsification* |  |  |
|  |  |  | *(12) Dont Détournement* |  |  |
|  |  | **(13) Dont sans authentification forte du client** |  |  |
|  |  |  | *(14) Dont Faux* |  |  |
|  |  |  | *(15) Dont Falsification* |  |  |
|  |  |  | *(16) Dont Détournement* |  |  |
|  |  |  | *(17)Dont au titre de l’Art. 11 de l’arrêté (Paiement sans contact de faible montant)* |  |  |
|  |  |  | *(18) Dont au titre de l’Art. 12 de l’arrêté (Automate transport / parking)* |  |  |
|  |  |  | *(19) Dont au titre de l’Art. 13 de l’arrêté (Bénéficiaire de confiance)* |  |  |
|  |  |  | *(20) Dont au titre de l’Art. 14 de l’arrêté (Opération récurrente)* |  |  |
|  |  |  | *(21) Dont au titre de l’Art. 15 de l’arrêté (Opération récurrente)* |  |  |
|  |  |  | *(22) Dont au titre de l’Art. 16 de l’arrêté (Faible montant)* |  |  |
|  |  |  | *(23) Dont au titre de l’Art. 17 de l’arrêté (Protocole de paiement sécurisé)* |  |  |
|  |  |  | *(24) Dont au titre de l’Art. 18 de l’arrêté (Analyse des risques)* |  |  |
|  |  | **(25) Dont virements traités en tant que virements instantanés** |  |  |

|  |  |  |
| --- | --- | --- |
|  |  | Total Valeur |
| (26) Pertes financières supportées par l’établissement déclarant |  |  |
| (27) Pertes financières supportées par le client émetteur |  |  |

Les données sur les virements instantanés ne seront à servir que si cette fonctionnalité est développée dans les systèmes de paiement locaux, et à partir du moment où elle aura été mise en production.

Les règles de contrôle suivantes doivent être appliquées :

|  |
| --- |
| En volume et en valeur et dans les différentes rubriques, le total de chaque indicateur est = à la somme des quatre sous-ventilations géographiques associées (Transactions effectuées dans la COM du déclarant + transactions effectuées dans une autre COM + Transaction effectuées en Métropole ou DOM e+ Transactions effectuées à l’étranger).Cette règle ne s’applique pas aux opérations fraudées réalisées sans identification forte du client sur la base d’une exemption listée dans l’arrêté du 14 janvier 2019. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur les virements émis par l’établissement est = à la somme de la fraude brute sur virements non électroniques initiés sur support papier, sur virements non électroniques initiés via un autre support et sur virements initiés par voie électronique. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude sur les virements initiés par voie électronique est = à la somme de la fraude sur virements initiés par lot / fichier, sur virements initiés depuis la banque en ligne, sur virements initiés depuis un GAB et sur virements initiés depuis une solution de paiement mobile. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude sur les virements initiés par voie électronique est = à la somme de la fraude sur virements initiés avec une authentification forte et de la fraude sur virements initiés sans authentification forte. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude sur les virements initiés par voie électronique avec une authentification forte du client est = à la somme de la fraude sur les virements correspondant aux typologies Faux, Falsification et Détournement initiés par voie électronique avec une authentification forte. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude sur les virements initiés par voie électronique sans authentification forte du client est = à la somme de la fraude sur les virements correspondant aux typologies Faux, Falsification et Détournement initiés par voie électronique sans authentification forte. |
| En volume et en valeur, et uniquement en Total, la fraude sur les virements initiés par voie électronique sans authentification forte du client est = à la somme de la fraude sur les virements initiés en application des exemptions prévues aux articles 11 à 18 de l’arrêté du 14 janvier 2019. |

### Virements faisant l’objet d’une demande de rappel de fonds (ONEGATE, écran « 2.2 – Virements faisant l’objet d’une demande de rappel de fonds »)

Il s’agit de déclarer, en nombre et valeur, les virements ayant fait l’objet d’une demande de rappel de fonds parmi les virements émis par l’établissement en tant que PSP du payeur (ou du donneur d’ordre) et sur les virements reçus en tant que PSP du payé (ou du bénéficiaire). Sont également précisés les retours de fonds effectivement réceptionnés après l’opération de recall en qualité de PSP du payeur et ceux acceptés par l’établissement en qualité de PSP du payé.

Remarques :

* Tous les types de virements sont concernés : virements locaux, virements SEPACOM, virements internationaux ;
* Les transactions visées sont les virements de clientèle (particuliers, professionnels, entreprises, administrations), quel que soit le mode d’échange utilisé pour la remise de l’ordre de virement. Sont exclus les virements entre IFM (Institutions Financières Monétaires) liés notamment au règlement d’opérations de marché, de trésorerie ou encore de compensation.
* **Données à déclarer :**

|  |  |  |
| --- | --- | --- |
|  | Volume en unités | Valeur enF CFP |
| (1) Virement faisant l’objet d’une demande de rappel de fonds (sur virements émis) |  |  |
|  | **(2) Dont opérations de retour de fonds réceptionnées après demande de rappel** |  |  |
| (3) Virement faisant l’objet d’une demande de rappel de fonds (sur virements reçus) |  |  |
|  | **(4) Dont opérations de retour de fonds acceptées après demande de rappel** |  |  |

Les règles de contrôle suivantes doivent être appliquées :

|  |
| --- |
| En volume et en valeur, les opérations de retour de fonds réceptionnées après demande de rappel sont < ou = aux virements faisant l’objet d’une demande de rappel de fonds (sur virements émis). |
| En volume et en valeur, les opérations de retour de fonds acceptées après demande de rappel sont < ou = aux virements faisant l’objet d’une demande de rappel de fonds (sur virements reçus). |

## CHEQUE

### Fraude brute sur les chèques reçus à l’encaissement par l’établissement (ONEGATE, écran « 3.1 – Fraude brute portant sur les chèques – établissement remettant »)

Il s’agit de déclarer, en nombre et valeur, la fraude sur les chèques reçus à l’encaissement par l’établissement en tant que PSP du payé (ou du remettant) avec une ventilation par typologie de fraude.

Remarques*:*

Sont inclus :

* Les chèques en F CFP, euros ou en devises ;
* Tous les types ou formes de chèques (chèque bancaire issu d’un carnet de chèque, lettre chèque), à l’exception des chèques de banque recensés par ailleurs.

Sont exclus :

* Les chèques tirés par l’établissement lui-même sur des comptes tenus par d’autres établissements, les chèques qu’il reçoit à son ordre sur ces mêmes comptes (dans ce cas, l’établissement agit en tant que client et ses opérations sont comptabilisées par son teneur de compte) ;
* Les chèques de banque ;
* Les chèques de voyage.
* **Typologie de fraude :**

|  |  |
| --- | --- |
| Vol, perte | -Utilisation par le fraudeur d’un chèque perdu ou volé à son titulaire légitime, revêtu d’une fausse signature qui n’est ni celle du titulaire du compte, ni celle de son mandataire.-Émission illégitime d’un chèque par un fraudeur utilisant une formule vierge (y compris lorsque l’opération a été effectuée sous la contrainte par le titulaire légitime). |
| Contrefaçon  | Faux chèque créé de toutes pièces par le fraudeur, émis sur une banque existante ou une fausse banque. |
| Falsification  | Chèque régulier intercepté par un fraudeur qui l’altère volontairement par grattage, gommage ou effacement. |
| Détournement, rejeu | -Chèque perdu ou volé après compensation dans les systèmes de paiement et présenté à nouveau à l’encaissement.-Chèque régulièrement émis, perdu ou volé, intercepté dans le circuit d’acheminement vers le bénéficiaire et encaissé sur un compte différent de celui du bénéficiaire légitime. La formule est correcte, le nom du bénéficiaire est inchangé et la ligne magnétique située en bas du chèque est valide, tout comme la signature du client. |

* **Arbre de décision sur le type de fraude au chèque :**

Les établissements qui le souhaitent pourront se référer à l’arbre de décision ci-dessous en cas de doute sur la classification de certains cas de fraude relatifs au chèque.



* **Données à déclarer :**

|  |  |
| --- | --- |
|  | Par zone géographique de localisation de la contrepartie (COM, Autres COM, France et Etranger) |
| (1) Fraude brute sur les chèques reçus à l’encaissement | Volume en unités | Valeur enF CFP |
| (2) Fraude brute sur les chèques – établissement remettant |  |  |
|  |  | (3) Dont fraude de type « vol, perte » |  |  |
|  |  | (4) Dont fraude de type « contrefaçon » |  |  |
|  |  | (5) Dont fraude de type « falsification »  |  |  |
|  |  | (6) Dont fraude de type « détournement, rejeu » |  |  |

|  |  |  |
| --- | --- | --- |
|  |  | Total Valeur |
| (7) Pertes financières supportées par l’établissement déclarant |  |  |
| (8) Pertes financières supportées par le client |  |  |

* **Contrôles :**

Les règles de contrôle suivantes doivent être appliquées :

|  |
| --- |
| En volume et en valeur, en total et dans les différentes rubriques, le total de chaque indicateur est = à la somme des quatre sous-ventilations géographiques correspondant à la localisation de la contrepartie (COM du déclarant, Autres COM, Métropole ou DOM et Etranger). |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur les chèques –établissement remettant- est = à la somme de la fraude brute de type « vol, perte », « contrefaçon », « falsification » et « détournement, rejeu » détectée par le déclarant en tant que PSP du remettant. |

### Fraude brute portant sur les chèques de banque – établissement remettant (ONEGATE, écran « 3.2 – Fraude brute portant sur les chèques de banque – établissement remettant »)

* **Données à déclarer :**

|  |  |
| --- | --- |
|  | Par zone géographique de localisation de la contrepartie (COM, Autres zone) |
|  | Volume en unités | Valeur enF CFP |
| (1) Fraude brute sur les chèques de banque – établissement remettant |  |  |
|  |  | (2) Dont fraude de type « vol, perte » |  |  |
|  |  | (3) Dont fraude de type « contrefaçon » |  |  |
|  |  | (4) Dont fraude de type « falsification »  |  |  |
|  |  | (5) Dont fraude de type « détournement, rejeu » |  |  |

* **Contrôles :**

Les règles de contrôle suivantes doivent être appliquées :

|  |
| --- |
| En volume et en valeur, et, par zone de sous-ventilations géographiques associées à la localisation de la contrepartie (COM et Autre zone –soit autres COM, Métropole ou DOM et Etranger), la fraude brute sur les chèques de banque –établissement remettant- est = à la somme de la fraude brute de type « vol, perte », « contrefaçon », « falsification » et « détournement, rejeu » détectée par le déclarant en tant que PSP du remettant. |

## PRELEVEMENT

### Fraude sur les prélèvements émis par l’établissement (ONEGATE, écran « 4.1 – Fraude brute sur prélèvements – banque émetteur »)

Il s’agit de déclarer, en nombre et en valeur, la fraude sur les prélèvements émis par l’établissement en tant que PSP du payé (ou du bénéficiaire) avec une ventilation par typologie de fraude, canal d’autorisation et zone géographique.

Remarques :

* Les prélèvements concernés sont les prélèvements locaux, SEPACOM ;
* Sont exclues les opérations de débit en compte dites « écritures en compte », pour lesquelles il n’existe pas d’autorisation de prélèvement ou de mandat et dont l’établissement teneur de compte est la contrepartie bénéficiaire (par exemple prélèvement de commissions, frais divers, débit pour remboursement de prêt effectué directement par l’établissement teneur de compte) ;
* Les prélèvements initiés par un créancier fraudeur sans mandat ou avec mandat créé de toute pièce sont à déclarer dans la rubrique « dont consentement donné par mandat papier ».
* **Typologie de fraude :**

|  |  |
| --- | --- |
| Faux | Le fraudeur créancier émet des prélèvements vers des numéros de compte qu’il a obtenus illégalement et sans aucune autorisation ou réalité économique sous-jacente. |
| Détournement | Le fraudeur débiteur usurpe l’identité et l’IBAN (international bank account number) d’un tiers pour la signature d’un mandat de prélèvement sur un compte qui n’est pas le sien.Les fraudes de type « Falsification » -ordres de prélèvement modifiés / altérés par le fraudeur- sont à intégrer parmi les fraudes de type « Détournement ». |

* **Arbre de décision sur le type de fraude au prélèvement :**

Les établissements qui le souhaitent pourront se référer à l’arbre de décision ci-dessous en cas de doute sur la classification de certains cas de fraude relatifs au prélèvement.

****

* **Canal d’autorisation :**

|  |  |
| --- | --- |
| Électronique | Internet + télématique. |
| Internet | Mandat de prélèvement émis depuis un canal internet (site de banque en ligne, site ou application mobile du créancier). |
| Télématique  | Mandat de prélèvement validé via d’autres canaux électroniques, hors site internet et application mobile de la banque ou du créancier. |
| Papier | Mandat de prélèvement collecté par un canal de type : courrier, formulaire, courriel, télécopie ou téléphone. Ces canaux ont en commun de nécessiter la re-saisie des instructions de paiement du payeur. |

* **zone géographique :**

|  |  |
| --- | --- |
| Prélèvement local | Prélèvement émis vers un PSP du payeur situé dans la collectivité du déclarant. |
| Prélèvement transfrontalier et intra COM du Pacifique | Prélèvement émis vers un PSP du payeur situé au sein d’une autre COM du Pacifique (hors COM du déclarant). |
| Prélèvement transfrontalier et hors COM du Pacifique  | Prélèvement émis vers un PSP du payeur situé en Métropole ou DOM. |

* **Données à déclarer :**

|  |  |
| --- | --- |
|  | Par zone géographique de localisation de la contrepartie (COM, Autres COM et métropole et DOM) |
|  | Volume en unités | Valeur enF CFP |
| (1) Fraude brute sur prélèvements émis par l’établissement |  |  |
|  | **(2) Dont prélèvements consentis par mandat électronique** |  |  |
|  |  | (3) Dont fraude de type « faux » (absence d’autorisation, …) |  |  |
|  |  | (4) Dont fraude de type « détournement » |  |  |
|  | **(5) Dont prélèvements consentis par mandat papier** |  |  |
|  |  | (6) Dont fraude de type « faux » (absence d’autorisation, …) |  |  |
|  |  | (7) Dont fraude de type « détournement » |  |  |

|  |  |  |
| --- | --- | --- |
|  |  | Total Valeur |
| (8) Pertes financières supportées par l’établissement déclarant |  |  |
| (9) Pertes financières supportées par le créancier |  |  |

* **Contrôles :**

Les règles de contrôle suivantes doivent être appliquées :

|  |
| --- |
| En volume et en valeur et dans les différentes rubriques, le total de chaque indicateur est = à la somme des trois sous-ventilations géographiques correspondant à la localisation de la contrepartie (COM du déclarant, Autres COM et Métropole ou DOM). |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur les prélèvements émis par l’établissement est = à la somme de la fraude sur les prélèvements consentis par mandat électronique et par mandat papier. |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur les prélèvements émis par l’établissement et consentis par mandat électronique est = à la somme des prélèvements fraudés de type « faux » et de type « détournement ». |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur les prélèvements émis par l’établissement et consentis par mandat papier est = à la somme des prélèvements fraudés de type « faux » et de type « détournement ». |

## LETTRE DE CHANGE RELEVE (LCR) – BILLET À ORDRE (BOR)

### Fraude sur la Lettre de Change Relevé (LCR) et le Billet à Ordre relevé (BOR) (ONEGATE, écran « 5.1 – Fraude brute portant sur les effets de commerce (LCR et BOR) »)

Il s’agit de déclarer, en nombre et en valeur, la fraude sur les effets de commerce émis et/ou reçus par l’établissement en tant que PSP du payé ou du remettant, avec une ventilation par typologie de fraude.

Remarques :

* Les LCR et BOR concernés sont les LCR et BOR payables dans les COM, en France et dans les DOM, libellés en F CFP ou en euros ;
* La date de référence à retenir est la date de règlement (et non la date de remise par le client).
* **Typologie de fraude :**

|  |  |
| --- | --- |
| Vol, perte | Émission illégitime d’un effet de commerce par un fraudeur en utilisant une formule vierge.  |
| Contrefaçon  | Faux effet de commerce créé de toutes pièces par le fraudeur, émis sur une banque existante ou une fausse banque. |
| Falsification  | Effet de commerce régulier intercepté par un fraudeur qui l’altère volontairement par grattage, gommage ou effacement. |
| Détournement, rejeu | Effet de commerce perdu ou volé après compensation dans les systèmes de paiement et présenté à nouveau à l’encaissement. |

* **Arbre de décision sur le type de fraude aux effets de commerce :**

Les établissements qui le souhaitent pourront se référer à l’arbre de décision ci-dessous en cas de doute sur la classification de certains cas de fraude relatifs aux effets de commerce.

|  |
| --- |
|  |

* **Données à déclarer :**

|  |  |
| --- | --- |
|  | Par zone géographique de localisation de la contrepartie (COM, Autres COM et Métropole ou DOM) |
|  | Volume en unités | Valeur enF CFP |
| (1) Fraude brute sur effets de commerce – établissement du remettant |  |  |
|  |  | (2) Dont fraude de type « vol, perte » |  |  |
|  |  | (3) Dont fraude de type « contrefaçon » |  |  |
|  |  | (4) Dont fraude de type « falsification »  |  |  |
|  |  | (5) Dont fraude de type « détournement, rejeu » |  |  |
| (6) Fraude brute sur effets de commerce – établissement du tiré ou du souscripteur |  |  |
|  |  | (7) Dont fraude de type « vol, perte » |  |  |
|  |  | (8) Dont fraude de type « contrefaçon » |  |  |
|  |  | (9) Dont fraude de type « falsification »  |  |  |
|  |  | (10) Dont fraude de type « détournement, rejeu » |  |  |

|  |  |  |
| --- | --- | --- |
| (11) Pertes financières supportées par l’établissement déclarant (en tant que banque du remettant) |  |  |
| (12) Pertes financières supportées par le remettant de l’effet de commerce (vue banque du bénéficiaire) |  |  |
| (13) Pertes financières supportées par l’établissement déclarant (en tant que banque du tiré) |  |  |
| (14) Pertes financières supportées par le tiré de l’effet de commerce (vue banque du tiré) |  |  |

* **Contrôles :**

Les règles de contrôle suivantes doivent être appliquées :

|  |
| --- |
| En volume et en valeur et dans les différentes rubriques, le total de chaque indicateur est = à la somme des trois sous-ventilations géographiques correspondant à la localisation de la contrepartie (COM du déclarant, Autres COM et Métropole ou DOM). |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur les effets de commerce – établissement du remettant est = à la somme des fraudes brutes sur effets de commerce remis à l’encaissement de type « vol, perte », « contrefaçon », « falsification » et « détournement, rejeu ». |
| En volume et en valeur, en total et par zone de sous-ventilations géographiques, la fraude brute sur les effets de commerce – établissement du tiré est = à la somme des fraudes brutes sur effets de commerce payés par les clients du déclarant, de type « vol, perte », « contrefaçon », « falsification » et « détournement, rejeu ». |