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

Card payment schemes fraud statistics

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

Observatory for the Security of Payment Means data collection

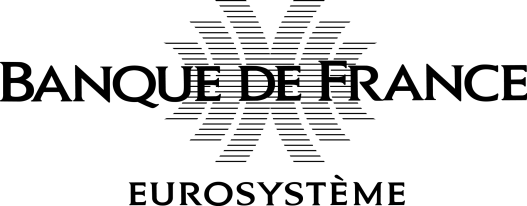
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**A guide to completion**

for survey declarants

**Applicable for data collected**

**as from H1 2023**



**Version History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comments** |
| 0.5 | 17/12/2020 |  |
| 0.6 | 14/01/2022 | Four subcomponents related to the indicator «Of which non-SLA payments » for remote payments |
| 0.7 | 15/02/2022 | Two definition amendments: “Of which, 3D Secure payments without strong authentication” and “o/w Transaction "One leg"” |
| 0.8 | 07/07/2023 | i) Exclusion of e-money card data  ii) Clarification of the definition of number of devices other than cards  iii) Adding the category “of which non 3D Secure payments with strong authentication”  iv) Clarification of the definition of “3D Secure payments with strong authentication”, “non 3 DS transactions and DSP2 non-compliant” et “non-authenticated payments”  v) Adding French Guyana to the appendice, which defines the French zone. |
|  |  |  |

**Foreword**

The Observatory’s guide to completion for its data collection takes into account the implementation of the EBA guidelines for French payment service providers since 1st January 2021. The main changes to the data collection process were:

* returns is required every six months;
* data will be broken down geographically by the following regions – France, abroad within the European Economic Area (EEA) and outside the EEA;
* transaction authentication methods will be monitored.

**1. Introduction**

Pursuant to Articles L. 141-4 and R. 141-1 of the *Code monétaire et financier* (the French Monetary and Financial Code), the Observatory for the Security of Payment Means is responsible for preparing harmonised payment means fraud statistics for publication within its annual report (the English language version is available at: <https://www.banque-france.fr/en/liste-chronologique/annual-activity-report>).

 To this end, the Banque de France, in its capacity as the secretariat of the Observatory, collects payment card data used to assess fraud on:

* domestic and international four-party card payment schemes operating in France for transactions carried out by their members; and
* domestic and international three-party card issuers operating in France.

This guide for completion provides all the information needed to correctly fill in the data collection. A glossary of terms used in the guide can be found in the appendix.

☞For the attention of institutions that issue both three and four-party cards: only data related to three-party cards should be declared; four-party cards data should be submitted by the appropriate four-party card scheme governance authority.

**2. An overview of the data collection process**

* ***Type of collected data***: the number and value of fraudulent transactions as well as the total number and value of all transactions performed in order to calculate the associated fraud rates. This includes all payments (face-to-face and remote) and withdrawals made using a payment card in France and abroad **when one of the counterparties to the transaction is considered to be French**: when the issuer is a French institution or the transaction is accepted in France (a merchant established or ATM located in France). Data on e-money cards, of which prepaid cards, are excluded of the collection.
* ***Presentation of collected data***: volumes should be presented in units and values should be presented in euro. If the source data is denominated in another currency, they should be converted into euro, preferably using the ECB’s published euro foreign exchange reference rates (*www.ecb.int*). Note that the ECB publishes conversion rates for each working day as well as monthly, quarterly and half-yearly averages.
* ***Reference date of collected data***: the date when the fraudulent transaction was carried out should be reported rather than the date when the fraud was detected or declared or when the card or card details were stolen.
* ***Geographical breakdown of collected data***: transaction and fraud data should be broken down into three distinct geographical regions: “France”, “Abroad within the EEA” (outside France) and “Abroad outside the EEA”. The breakdown is based on the country where the card issuer and the transaction acceptor (merchant or ATM), respectively, are located, **without duplication**, in order to avoid double counting of transactions or fraud. The scope of the “France” and “EEA” regions are defined in the appendix.
* ***Fraud assessment:***
  + ***Defining fraud:***

|  |
| --- |
| Fraud is defined as the illegitimate use of a payment card or its related data and any act that contributes to the preparation for their illegitimate use and/or effective illegitimate use:   * **that cause financial harm:** to the account-holding institution, be it the bank of the cardholder or of the acceptor (e.g. merchant or general government agency, on its own account or within a payment scheme), the cardholder, acceptor, issuer, insurer, trusted third party or any party involved in the chain of design, manufacture, transport, or distribution of physical or logical data that could incur civil, commercial or criminal liability; * **by whatever means:**   + the methods used to obtain, without lawful reason, cards or the data stored on them (theft, taking possession of cards or devices, physical or logical data and personalisation data and/or misappropriation of secret codes and/or security codes, hacking of magnetic stripes and chips, etc.),   + the procedures for using cards or the data stored on them (face-to-face or remote payments or withdrawals, via physical use of the card or the card number, via UPTs, etc.),   + the geographical region of the issue or use of the cards or the data stored on them,   + the type of payment card ; * **and irrespective of the identity of the fraudster:** a third party, the account-holding bank, the cardholder her/himself (for example, using the card after it has been declared lost or stolen, or wrongfully contesting transactions), the acceptor, the issuer, an insurer, a trusted third party, etc. |

* + ***A “gross fraud” approach:*** fraud should be assessed using a gross fraud approach (in contrast to a “net fraud” approach), which involves taking into account (i) all authorised transactions, (ii) that are subsequently rejected as being fraudulent, and (iii) the initial transaction amounts without taking into account any measures subsequently taken by the counterparties to reduce the related loss. Attempted fraud or fraudulent activities prevented before a transaction can be concluded should not be declared.

**3. Timetable and submission of collected data**

* ***Timetable****:* Data are collected on a half-yearly basis during the following periods:
* for the first half of the year (January to June), from the first working day in August to the last working day in October;
* for the second half of the year (July to December), from the first working day in February to the last working day in April of the following year.

Declarants are informed directly when the collection periods are open by the secretariat of the Observatory for the Security of Payment Means (OSMP for *Observatoire de la Sécurité des moyens de Paiements*).

* ***Declaration procedures***: declarations are submitted via the OneGate-Oscamps portal operated by the Banque de France. Terms of access for the portal are set out in the ONEGATE external user manual.

An interface agreement is provided with this guide.

All the technical documents are available on the Banque de France website: <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>

An excel version of the questionnaire is also available via this document:



**For further information, please contact the Banque de France division tasked with providing the secretariat of the OSMP using the contact details below:**

|  |
| --- |
| DIRECTORATE GENERAL OF MEANS OF PAYMENT  Directorate of the Study and Oversight of Payments  Cashless Means of Payment Division  S2B-2323  75049 PARIS CEDEX 01  [2323-OSMP-UT@banque-france.fr](mailto:2323-OSMP-UT@banque-france.fr) |

**4. Questionnaire structure and content**

The questionnaire is structured as follows:

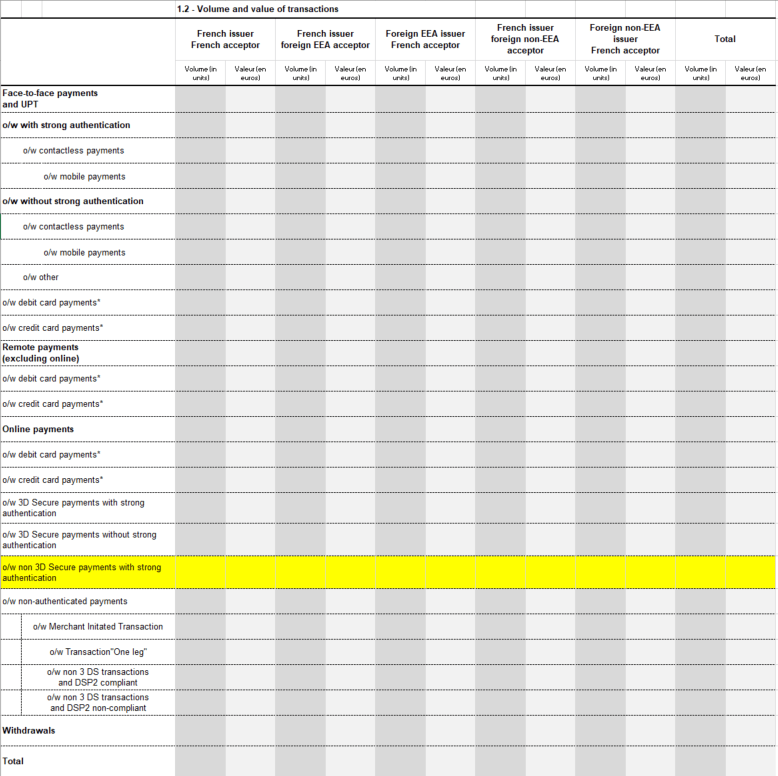
* Section 1.1 – Number of cards: data on the amount of cards in circulation and cards declared stolen or lost.
* Section 1.2 – Volume and value of transactions: the number and value of transactions broken down by transaction type, authentication method, and geographical region of the card issuer and transaction acceptor.
* Sections 2.a to 2.e – Breakdown of fraud: source of fraud: for each geographical region of the card issuer and transaction acceptor, the number and value of fraudulent transactions broken down by transaction type, authentication method, card function and type of fraud.
* Section 3.1 – Breakdown of domestic transaction fraud on remote sales by sector of activity: domestic fraud on remote payments broken down by the merchant’s sector of activity.

**Section 1.1 – Number of cards**

|  |  |  |
| --- | --- | --- |
| **1.1 – Number of cards** | | |
| Number of cards issued in France and valid as at the end of the half year under review |  | cards |
| *o/w dual interface chip cards (allowing contactless and non-contactless payments)* |  | cards |
| Number of devices (other than cards like smartphones or connected devices) enabling contactless payments and valid as at the end of the half year under review. The number of tokens associated with such devices can be used for making an estimation of this indicator. |  | devices |
| Number of cards and other devices reported lost or stolen during the half year under review and used for at least one recorded fraudulent transaction |  | cards and devices |

* **Cards:** payment cards. Cards that are not authorised to make payments and that can only be used to make withdrawals from the issuing institution’s ATMs are excluded and e-money cards.
* **Specific rules to avoid double counting or omissions applicable to institutions that issue co-badged cards (CB-Mastercard or CB-Visa):**
* **GIE-CB**: all “CB” cards, including co-badged CB-Mastercard and CB-Visa should be declared in Section 1.1;
* **Mastercard and Visa**: only “*Mastercard only*” and “*Visa only*” cards should be declared in Section 1.1 ; co-badged CB-Mastercard and CB-Visa should be here excluded.

**Section 1.2 – Volume and value of transactions**



* **Transaction type:**

|  |  |
| --- | --- |
| **Face-to-face payments and UPT** | Payments made at a point of sale or at an unattended payment terminal (UPT), including contactless payments. |
| Of which, payments with strong authentication | Face-to-face payments by card authorised using a strong authentication method, such as “Chip and PIN” payments or payments with PIN Online verification, using a biometric bank card or by mobile devices with biometric sensors, mPIN entry or passwords. |
| Of which, payments without strong authentication | Face-to-face payments by card without strong authentication, including magnetic strip card or chip card payments with a written signature, contactless payments without biometric or PIN online verification, or mobile payments without authentication via an inherence factor (through biometric sensors) or a knowledge factor (password). |
| Of which, contactless payments | Face-to-face payments using the card’s contactless function. |
| Of which, mobile payments | Face-to-face payments using a mobile device (telephone, tablet, connected smartwatch, etc.) to initiate a payment order through contactless technologies, such as NFC, Bluetooth, 1D or 2D barcodes, etc., and potentially to arrange money transfers. The most commonly known include Apple Pay, Samsung Pay, Google Pay, Lyf Pay and Paylib contactless payment.  💣“Mobile payments” are a sub-category of “contactless payments”. |
| Of which, other | Payments at parking pay points or motorway toll booths, for example, by swiping the card’s magnetic stripe. |
| **Remote payments (excluding online)** | Payments made by post or email or by telephone or fax (mail order/telephone order). |
| **Online payments** | Payments made on the internet (on a merchant’s site or through an application). |
| Of which, 3D Secure payments with strong authentication | Payments made on the internet via a 3D Secure infrastructure (or equivalent) with a strong cardholder authentication arrangement. This category can include payments, where the issuer has outsourced the provision and verification of the SCA to a third party in compliance with the requirements in PSD2 and EBA Guidelines on outsourcing arrangements (ex: digital wallet provider, merchant etc.). |
| Of which non 3D-Secure payments with strong authentication | Online payments without using 3D-secure protocol (or equivalent). The provision and verification of the SCA is outsourced to a third party in compliance with the requirements in PSD2 and EBA Guidelines on outsourcing arrangements (ex: digital wallet provider, merchant etc.). |
| Of which, 3D Secure payments without strong authentication | Payments made on the internet via a 3D Secure infrastructure without a strong cardholder authentication arrangement (i.e. by applying a predefined PSD2 exemption or in the event of an incident preventing 3D Secure implementation). That category includes 3D secure payments relying on a single element of authentication (e.g. SMS-OTP only). |
| Of which non-authenticated payments | Online payments made without using the 3D Secure protocol (or equivalent) and without any SCA. |
| o/w Merchant Initiated Transactions | Payments initiated by the payee, without any direct involvement of the cardholder, based on a pre-existing agreement between the payer and the payee (“MIT mandate”) such as subscriptions, payments in several instalments or payment with unknown amount based on consumption. When payments are both MIT and one leg, they should be considered as MIT. |
| o/w "one leg" transactions | Non 3D-Secure payments in which the PSP of the payer or the payee is located outside the European Economic Area (EEA). |
| o/w non 3 DS transactions  and DSP2 compliant transactions | Payments presenting a predefined PSD2 exemption flag within the authorization flow (e.g  Direct to Authorization – DTA involving an exemption factor). |
| o/w non 3 DS transactions  and DSP2 non-compliant transactions | Non 3D-Secure Payments that are within the scope of the PSD2 but that do not present any PSD2 exemption flag and for which the authorization is granted. That category includes payments that involve both a European payee and a non-EEE acquirer. In the case of a “one leg” and “non 3 DS transactions and DSP2 non-compliant transactions”, the transaction has to be classified as a “one leg” transaction. |
| **Withdrawals** | Cash withdrawals at ATMs. |

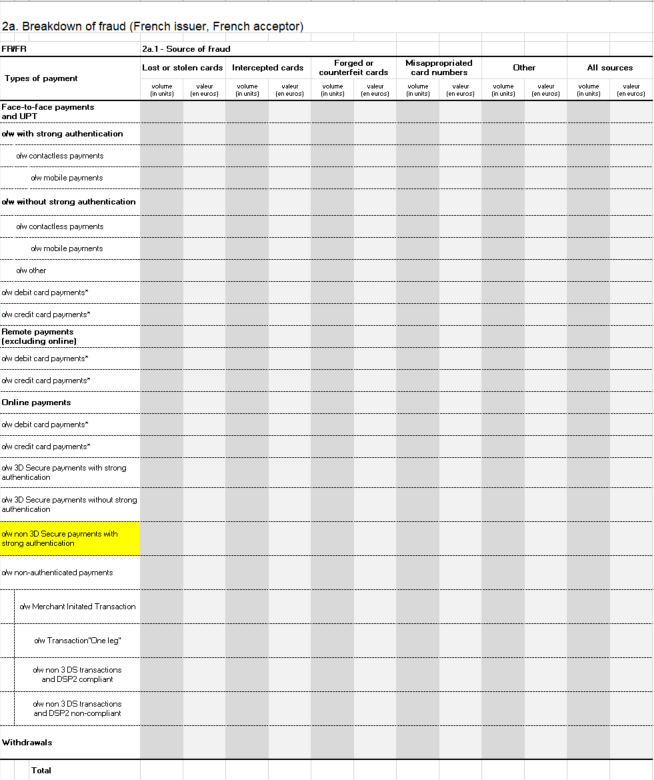
* **Card type:**

|  |  |
| --- | --- |
| Debit card | Immediate debit cards. |
| Credit card | Credit cards and deferred debit cards. |

Note: in the case of commercial cards, if the institution cannot ascertain the function of the card, it should be categorised as a credit card by default.

* **Specific rules to avoid double counting or omissions applicable to institutions that issue co-badged cards (CB-Mastercard or CB-Visa):**
* **GIE-CB**: declaration of transactions processed by the “CB” system only (irrespective of whether the card used is “CB only” or co-badged);
* **Mastercard and Visa**: declaration of transactions processed[[1]](#footnote-1) by the Mastercard system or Visa system only (irrespective of whether the card used is “Mastercard only”, “Visa only” or co-badged).

**Sections 2.a.1 to 2.d.1 – Breakdown of fraud**



* **Source of fraud:**

|  |  |
| --- | --- |
| Lost or stolen cards | The fraudster uses a lost or stolen credit card, without the lawful cardholder’s knowledge. |
| Intercepted cards | The card is intercepted when the issuer sends it to the lawful cardholder. This type of fraud is similar to card loss or theft except that it is difficult for the lawful cardholders to ascertain that a fraudster is in possession of a card that belongs to them. In such cases, the fraudster seeks to exploit vulnerabilities in the procedures used to send cards. |
| Forged or counterfeit cards | Falsification of a payment card consists in modifying an authentic card’s magnetic strip data, embossing[[2]](#footnote-2) or programming. Counterfeiting a card means creating an object that appears to be an authentic payment card and/or is capable of deceiving an unattended payment terminal (UPT) or a merchant’s payment terminal. In both cases, the fraudster endeavours to create a card that incorporates the data required to deceive the acceptance system. |
| Misappropriated card numbers | A cardholder’s card number is taken without his or her knowledge or created through card number generation,[[3]](#footnote-3) and used in remote transactions. |
| Other | Any other fraud method, such as the use of a card number (or personal account number – PAN) that is consistent but yet not attributed to a cardholder and then used in remote transactions, the fraudulent modification of a legitimate payment order, manipulation of a payer to obtain a payment by card, etc. |

* **Specific rules to avoid double counting or omissions applicable to institutions that issue co-badged cards (CB-Mastercard or CB-Visa):**
* **GIE-CB**: declaration of fraudulent transactions processed4 by the “CB” system only (irrespective of whether the card used is “CB only” or co-badged);
* **Mastercard and Visa**: declaration of fraudulent transactions processed[[4]](#footnote-4) by the Mastercard system or Visa system only (irrespective of whether the card used is “Mastercard only”, “Visa only” or co-badged).

**Section 5.1 – Breakdown of domestic transaction fraud on remote sales by sector of activity (FR issuer/FR acceptor)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | Transactions | | Fraud | | Fraud rate (%) |
| volume (in units) | value  (in euro) | volume (in units) | value  (in euro) |
| General and semi-general trade | |  |  |  |  |  |
| Technical and cultural products (books, dvds, computer, hi-fi, photography and video equipment, household appliances, etc.) | |  |  |  |  |  |
| Travel and transportation | |  |  |  |  |  |
| Telephony and communication | |  |  |  |  |  |
| Foodstuffs | |  |  |  |  |  |
| Household goods, furnishings and DIY | |  |  |  |  |  |
| Insurance | |  |  |  |  |  |
| Health, beauty and personal care | |  |  |  |  |  |
| Personal and professional services | |  |  |  |  |  |
| Account loading and person-to-person sales | |  |  |  |  |  |
| Online gaming | |  |  |  |  |  |
| Miscellaneous | |  |  |  |  |  |
| Total | |  |  |  |  |  |
|  | **5.2 - Additional comments** | | | | | |
|  | | | | | | |

The data collected concerns remote sales and domestic payments (French issuers and merchants) only.

The following examples are provided to help clarify merchant classifications.

|  |  |
| --- | --- |
| General and semi-general merchants | 3suisses.fr, amazon.fr, auchan.fr, cdiscount.com, laredoute.fr, m6boutique.com, mistergooddeal.com, quelle.fr, vente-privee.com, vertbaudet.fr |
| Technical and cultural products (books, dvds, computer, hi-fi, photography and video equipment, household appliances, etc.) | alapage.com, , darty.com, fnac.com, franceloisirs.com, ldlc.com, pixmania.com, rueducommerce.fr, topachat.com |
| Travel and transportation | accorhotels.com, airfrance.fr, anyway.com, avis.fr, expedia.fr, nouvelles-frontieres.fr, opodo.fr, vivacances.fr, voyagesloisirs.com, voyages-sncf.com. |
| Telephony and communication | bouyguestelecom.fr, free.fr, orange.fr, sfr.fr |
| Foodstuffs | auchandirect.fr, houra.fr, ooshop.com, monoprix.com, telemarket.fr |
| Household goods, furnishings and DIY | but.fr, castorama.fr, conforama.fr, ikea.fr, leroymerlin.fr |
| Insurance | europ-assistance.fr, mondial-assistance.fr |
| Health, beauty and personal care | ccbparis.fr, sephora.fr, yves-rocher.fr |
| Account loading and person-to-person sales | ebay.fr, rakuten.com |
| Personal and professional services | 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 |
| Online gaming | fdjeux.com, pmu.fr, betclic.fr |

The following Merchant Category Code (MCC) list can be used to help classify merchants in their correct categories:



**5. Appendix**

**Glossary**

|  |  |
| --- | --- |
|  | **> Acceptor** |
|  | Any merchant, service provider and, more generally, legal entities or individuals under private or public law receiving funds in payment by card and having signed an acceptance agreement with their bank or card management body to this end. |
|  | **> Acquirer** |
|  | Credit institutions, institutions and services referred to in Article L. 518-1 of the French Monetary and Financial Code that are contractually bound to the acceptor and acquire data related to the transactions performed. The acquirer is notably responsible for collecting the transactions and settlements of acceptors, within the limits of the agreements in force. |
|  | **> Counterfeit card** |
|  | For UPT transactions: a card equipped with the data needed to fool the system. |
|  | For face-to-face transactions: a card manufactured with more or less the same visual appearance, including security features, as an authentic card with real cardholder data, and designed to deceive an acceptor. |
|  | **> Payment card** |
|  | The concept of a payment card is defined in Article L. 132-1 of the French Monetary and Financial Code as: |
|  | “any card issued by a credit institution or by an institution or service referred to in Article L 518-1 that enables its holder to withdraw or transfer funds”. |
|  | **> Issuer** |
|  | An organisation or its agent that has issued a payment card to a cardholder and is contractually bound to that cardholder. |
|  | **> Misappropriated card number** |
|  | A cardholder’s card number taken without his or her knowledge or created through card number generation, and used in remote transactions. |

**Glossary**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **France**   |  | | --- | | Metropolitan France | | Overseas departments and regions:[[5]](#footnote-5) | | Guadeloupe | | Martinique | | Réunion | | Saint Pierre and Miquelon | | Mayotte | | Saint Barthélemy | | Saint Martin | | French Guyana | | The Principality of Monaco | | **EEA countries (outside France)**   |  |  | | --- | --- | | Germany | (DE) | | Austria | (AT) | | Belgium | (BE) | | Bulgaria | (BG) | | Cyprus | (CY) | | Croatia | (HR) | | Denmark | (DK) | | Spain | (ES) | | Estonia | (EE) | | Finland | (FI) | | Greece | (EL) | | Hungary | (HU) | | Ireland | (IE) | | Iceland | (IS) | | Italy | (IT) | | Latvia | (LV) | | Liechtenstein | (LI) | | Lithuania | (LT) | | Luxembourg | (LU) | | Malta | (MT) | | Norway | (NO) | | Netherlands | (NL) | | Poland | (PL) | | Portugal | (PT) | | Czech Republic | (CZ) | | Romania | (RO) | | Slovenia | (SI) | | Slovakia | (SK) | | Sweden | (SE) | |

1. In the sense of authorised and cleared. [↑](#footnote-ref-1)
2. Modification of the raised numbers printed to form the card number. [↑](#footnote-ref-2)
3. A technique that consists in using issuers’ own rules for creating payment card numbers to generate fraudulent numbers. [↑](#footnote-ref-3)
4. In the sense of authorised and cleared. [↑](#footnote-ref-4)
5. Other overseas collectivities (French Polynesia, Wallis and Futuna) and New Caledonia, which are not members of the European Union, are excluded from the “France” region. [↑](#footnote-ref-5)