



INSTRUCTIONS FOR PAYMENT AND FRAUD DATA REPORTING (MAPE)

Version: 1.5
Date: 25.11.2024
Valid from: 1.7.2024
Application: 1.7.2024



Version history

Version	Date	Valid from	Changes
1.0	28.5.2021	1 January 2022	First version of reporting instructions.
1.1	8.9.2021	1 January 2022	<ul style="list-style-type: none"> - The number of records to be reported by the full reporters updated in chapter 2.4 - ACCO record: <ul style="list-style-type: none"> • Modified phrasing • Definition of "Client funds (A030)" in field 4 clarified • Definition of "Deposit other than an overnight deposit (NOD)" in field 5 clarified - HPAY record: <ul style="list-style-type: none"> • Definition of "Fraudulent payment transaction (FT)" in field 5 clarified • Definitions of "Direct debit (DD)", "Credit to the account by simple book entry (CBE)" and "Debit from the account by simple book entry (DBE)" in field 6 clarified • Definition of field 8 clarified • Definition of "Other (OTH)" in field 11 clarified • Definition of field 15 and its category "Non-remote (NR)" clarified • Definition of field 17 and its category "ATM (T020)" clarified • Definition of field 18 and its categories "PISP (PI)" and "Mobile payment solution (MP)" clarified - QPAY record: <ul style="list-style-type: none"> • Definition of "Direct debit (DD)" in field 6 clarified • Definition of field 8 clarified • Definition of field 15 and its category "Non-remote (NR)" clarified • New sub-heading 7.9 added - APAY record: <ul style="list-style-type: none"> • Definition of "Fraudulent payment transaction (FT)" in field 5 clarified • Definitions of "Direct debit (DD)", "Credit to the account by simple book entry (CBE)" and "Debit from the account by simple book entry (DBE)" in field 6 clarified • Definition of field 8 clarified • Definition of field 15 and its category "Non-remote (NR)" clarified • Definition of field 17 and its category "ATM (T020)" clarified - SERV record: <ul style="list-style-type: none"> • Definition of "Online invoices sent (S070)" clarified



1.2	28.12.2021	1 January 2022	<ul style="list-style-type: none"> - General instructions for avoidance of double reporting in chapter 2.2 amended - CARD record: <ul style="list-style-type: none"> • Definition of “Delayed debit card C120” clarified (affects records HPAY and APAY) - HPAY record: <ul style="list-style-type: none"> • Examples on reporting of field 6 “Credit transfer (CT)” added. Also applies to records QPAY and APAY. • Definition of field 11 item “Correspondent banking payment (CRBP)” clarified. • Definition of field 11 item “Other (OTH)” clarified. • Definition of field 12 “Instant payments” clarified • Possible roles of a payment service provider in credit transfers and direct debits changed. - QPAY record: <ul style="list-style-type: none"> • Possible roles of a payment service provider in credit transfers and direct debits changed. - APAY record: <ul style="list-style-type: none"> • Possible roles of a payment service provider in credit transfers and direct debits changed. - SERV record: <ul style="list-style-type: none"> • Definition of item “Online invoices sent (S070)” clarified. • Definitions of items "Customer identification transactions (S010)", "Electronic bank statements (KTO) (S021)", "ISO20022 bank statements (XML) (S022)", "Online invoice receiver agreements (S061)", "Online invoice sender agreements (S062)" and "SDD agreements by creditors (S063)" clarified.
1.3	16.12.2022	1 January 2023	<ul style="list-style-type: none"> • Chapter 1.3 <i>ECB's minimum requirements and sanctions</i> added. • Chapter 2.3 <i>Payment service provider's role</i>: definition of PSP clarified. - ACCO record: <ul style="list-style-type: none"> • Clarified whether each reportable item is stock or flow data. • Reference periods for items A010, A022, A023, A024 and A025 in field 4 revised from a calendar year to reporting period. • Reporting instructions for country of location concerning item “Payment accounts accessed by AISPs (A021)” clarified. - APAY record: <ul style="list-style-type: none"> • Chapter 6.1 <i>Reporter's role (field 4)</i>: definitions of payment intermediary and payment processor elaborated. • Chapter 6.2 <i>Information type (field 5)</i>: definition of fraudulent payment transaction clarified. • Chapter 6.3 <i>Payment service (field 6)</i>: Definitions of the following field 6 items clarified: "Credit transfer (CT)", "Direct



			<p>debit" (DD), "Card payment" (CP), "Cash withdrawal" (CW) and "Electronic money payment" (EMP).</p> <ul style="list-style-type: none"> • Chapter 6.4 <i>Electronic (field 8)</i>: Definition of field 8 "Electronic" clarified • Chapter 6.10 <i>Reason for non-SCA (field 21)</i>: Reporting instructions for field 21 clarified.
1.4	19.6.2023	1 January 2024	<ul style="list-style-type: none"> • Chapter 1.3.2 Infringement monitoring added - CARD record: <ul style="list-style-type: none"> • "Diner's Club (DINE)" added as an option in field 6 Payment Scheme. - APAY record: <ul style="list-style-type: none"> • Examples added to the reporting of field 6 "Credit Card payment (CP)". • "E-money card loading or unloading (EML)" added as an option in field 6 Payment Service. Modified descriptions of field 6 Payment Service. • "Refunded card payment (RCP)" added as an option in field 6 Payment Service. • Chapter 6.7 <i>Remote/non-remote payment (field 15)</i>: Definition "Remote payment (R)" clarified.
1.5	25.11.2024	1 July 2024	<ul style="list-style-type: none"> • References to csv reporting have been replaced by terms applicable to xml reporting format.



CONTENTS

1 Introduction	6
1.1 Basis of payment statistics reporting and purpose of use of the data	6
1.2 Reporting population and granting of derogations	7
1.3 ECB's minimum requirements, monitoring and sanctions	9
1.3.1 ECB's minimum requirements	9
1.3.2 Infringement monitoring	10
2 General instructions.....	11
2.1 Data to be reported	11
2.2 Payment transactions.....	11
2.3 Payment service provider's role	13
2.4 Record sections to be reported	14
2.5 Schedule of submission of fraud and payment data to Bank of Finland.....	16
2.6 Reporter's obligation to retain reported data	16
3 Accounts, deposits and offices (ACCO record section).....	17
3.1 Accounts, deposits and offices (element accountsDepositsAndOffices)	17
3.2 Deposit type (element depositType).....	20
3.3 Assets transferable via network (element assetsTransferableViaNetwork).....	21
3.4 E-money account (element eMoneyAccount).....	21
3.5 Payment service user (element paymentServiceUser)	22
3.6 Country (element country).....	22
4 Number of cards (CARD record section)	23
4.1 Card type (element cardType).....	23
4.2 E-money card type (element eMoneyCardType)	25
4.3 Scheme (element scheme)	25
4.4 Cash function (element cashFunction)	26
4.5 Combination card (element combinationCard)	26
4.6 Card technology (element cardTechnology).....	26
4.7 Payment service user (element paymentServiceUser)	27
4.8 Country (element country).....	27
5 Number of terminals (TERM record section).....	28
5.1 Terminal type (element terminalType).....	28
5.2 EFTPOS (element eftpos).....	28
5.3 Contactless payment (element contactlessPayment)	29
5.4 Terminal accepting e-money (element terminalAcceptingEMoney)	29
5.5 E-money loading/unloading (element eMoneyLoadingUnloading)	29
5.6 Country (element country).....	29
6 Annual reporting of payment transactions and fraudulent payment transactions (APAY record section)	30
6.1 Reporter's role (element reportersRole)	30
6.2 Information type (element informationType)	31
6.3 Payment service (element paymentService)	32
6.4 Electronic (element electronic)	42
6.5 Channel for giving consent (element channelForGivingConsent)	42
6.6 Card type (element cardType).....	43
6.7 Remote/non-remote (element remoteNonRemote)	44
6.8 Terminal (element terminal)	45
6.9 Customer authentication (element customerAuthentication).....	45
6.10 Reason for non-SCA (element reasonForNonSCA)	45



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

6.11 Fraud type (element fraudType)	47
6.12 Liability bearer (element liabilityBearer).....	48
6.13 Counterparty's PSP location (element counterpartyPSPLocation).....	49
6.14 Terminal location (element terminalLocation)	49



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

1 INTRODUCTION

1.1 Basis of payment statistics reporting and purpose of use of the data

The Bank of Finland collects data from payment service providers and payment system operators in the payment and fraud data collection (MAPE data collection) for the conduct of the duties of the European System of Central Banks (ESCB) and the Bank of Finland as well as other national purposes. The data is used, for example, to monitor the development of payment instruments and services, in payment systems oversight, monitoring of fraud related to payment services, monitoring of cross-border trade and preparation of economic forecasts. The Financial Supervisory Authority uses the data in the supervision of payment service providers and payment system operators. The Bank of Finland releases the data to Statistics Finland for the compilation of statistics, and to Finance Finland based on letters of attorney. The data are forwarded via the ECB to the European Banking Authority (EBA). The data may also be disclosed to other national authorities where they have a statutory right to obtain the data concerned. The data may also be used for other statistical purposes and on an anonymised basis for research purposes. The right of the Bank of Finland to disclose information is based on the Act on the Bank of Finland (214/1998, section 26). Statistics compiled by the Bank of Finland are made public e.g. on the websites of the Bank of Finland and the European Central Bank.

The Bank of Finland's authority to obtain information is based on the European Union Regulation concerning the collection of statistical information by the European Central Bank (ECB) (EU No 2533/98, as amended by 2015/373) and sections 26 and 28 of the Act on the Bank of Finland (214/1998).

The payment and fraud data collection is based on the ECB Regulation on payment statistics (ECB/2013/43, as amended by ECB/2020/59, hereinafter *Regulation*) and Guidelines on payment statistics (ECB/2021/13, hereinafter *Guidelines*). In addition, data based on the Act on Payment Institutions (297/2010) and the Credit Institutions Act (610/2014) is collected in the MAPE data collection.

A credit institution providing payment accounts must report to the FIN-FSA in accordance with chapter 15 a, section 6 of the Credit Institutions Act (610/2014, as amended by 1054/2016 and 448/2017). Under section 9 a of the Payment Institutions Act, a similar reporting obligation also applies to payment institutions.

MF reporting is based on section 19 b of the Payment Institutions Act, which also applies to credit institutions under chapter 9, section 16(4) of the Credit Institutions Act (610/2014). The collection of data for ML reporting is based on section 18(2) of the Act on the Financial Supervisory Authority (878/2008), based on which data is collected for the purposes laid out in section 7(2)(7) and 7 a(1) of the Payment Institutions Act.



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

These data are collected in the MAPE data collection. The MAPE data collection replaces the Bank of Finland's MATI data collection. The MAPE data collection also replaces the FIN-FSA's MF reporting (reporting of fraud data related to payment services), which is based on Directive (EU) 2015/2366 (the revised Payment Services Directive, PSD2, hereinafter *Payment Services Directive*) and Guidelines of the European Banking Authority issued thereunder. In addition, the MAPE data collection replaces the FIN-FSA's ML reporting (total number of payment transactions) for registered payment service providers operating without authorisation.

Statistical regulations are always binding on the reporters, and by virtue of Article 7 of Regulation 2533/98, the ECB may impose sanctions on reporters which fail to comply with the reporting obligation.

1.2 Reporting population and granting of derogations

The actual reporting population in the MAPE data collection consists of payment service providers (incl. issuers of electronic money) and payment system operators. In Finland, these comprise:

- Domestic credit institutions
- Branches of foreign credit institutions in Finland
- Domestic payment institutions
- Branches of foreign payment institutions in Finland
- Domestic registered institutions i.e. legal and natural persons providing payment service without authorisation.

In accordance with the ECB Regulation on payment statistics, all entities included in the actual reporting population are under the reporting obligation. However, by virtue of Article 4, paragraphs 2 and 3 of the Regulation, the national central bank may grant reporting concessions (derogation). In payment and fraud reporting, this means lighter reporting once a year. Hence, it is not possible to have a full exemption from the reporting. Institutions subject to complete reporting are called full reporters and those subject to lighter reporting with derogations are called tail reporters.

A reporter may be given a derogation if it is a small reporter **and** full national data collection covers a sufficient proportion of the total value of payment services provided by the payment service providers in the member state, by payment service.

The following are considered small reporters:

1. Domestic registered institutions i.e. legal and natural persons providing payment service without authorisation.
2. Other payment service providers (e.g. credit institutions) if they meet the conditions laid down in Article 32(1) and (2) of the Payment Services Directive and Article 9(1) and (2) of Directive 2009/110/EC, i.e:



- the monthly average of the preceding 12 months' total value of payment transactions executed by the person concerned (including any agent) amounts to no more than EUR 3 million **and**
- the total business activities generate an average outstanding electronic money that amounts to no more than EUR 5,000,000

Full national data collection must demonstrate adequate comprehensiveness:

- a) The total contribution of payment service providers subject to derogations may not exceed 5% of the total value of each of the following payment services at the national level:
- i. Credit transfers (sent),
 - ii. Direct debits (sent),
 - iii. Card-based payment transactions (sent and received),
 - iv. Card withdrawals,
 - v. Electronic money payments (sent),
 - vi. Cheques (sent),
 - vii. Money remittances (sent),
 - viii. Other payment services included in the Payment Services Directive (sent),
 - ix. Payment initiation services,
 - x. Other payment services not included in the Payment Services Directive (sent),
 - Includes, for example account credits/debits by simple account entry.
- b) The total number of account information service providers (AISP) with a derogation may amount to no more than 5% at the national level.

In February 2021, the Bank of Finland notified all reporters of the reporting obligation and its scope. The basis of reporting derogations and the coverage of full reporting are checked annually based on the previous calendar year's payment and fraud data. Changes in the reporting obligation, that is, beginning or end of a derogation, are notified separately, leaving the reporter enough time to prepare for the change.



1.3 ECB's minimum requirements, monitoring and sanctions

1.3.1 ECB's minimum requirements

Reporting agents must fulfil the following minimum standards to meet the European Central Bank's (ECB's) statistical reporting requirements.

1. Minimum standards for transmission:
 - a) reporting must be timely and within the deadlines set by the relevant NCB;
 - b) statistical reports must take their form and format from the technical reporting requirements set by the relevant NCB;
 - c) the reporting agent must provide the details of one or more contact persons to the relevant NCB;
 - d) the technical specifications for data transmission to the relevant NCBs must be followed.
2. Minimum standards for accuracy:
 - a) statistical information must be correct: all linear constraints must be fulfilled (e.g. subtotals must add up to totals), and data must be consistent across all frequencies;
 - b) reporting agents must be able to provide information on the developments implied by the transmitted data;
 - c) statistical information must be complete and must not contain continuous and structural gaps; existing gaps must be acknowledged, explained to the relevant NCB and, where applicable, bridged as soon as possible;
 - d) reporting agents must follow the rounding policy set by the relevant NCB for the technical transmission of the data.
3. Minimum standards for compliance with concepts:
 - a) statistical information must comply with the definitions and classifications contained in this Regulation;
 - b) in the event of deviations from these definitions and classifications reporting agents must monitor and quantify the difference between the measure used and the measure contained in this Regulation on a regular basis;
 - c) reporting agents must be able to explain breaks in the transmitted data compared with the previous periods' figures.
4. Minimum standards for revisions:

The revisions policy and procedures set by the ECB and the relevant NCB must be followed. Revisions deviating from regular revisions must be accompanied by explanatory notes.

If the data provider does not meet the minimum requirements for transmission, accuracy, compliance with concepts and revisions laid down in Annex IV of Regulation ECB/2013/43, amended ECB/2020/59), the ECB may impose sanctions on the data provider under Regulation EU No 2533/98, as amended by 2015/373).



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

1.3.2 Infringement monitoring

The ECB has established a non-compliance system for monitoring infringements concerning the reporting of statistical data under all ECB regulations or decisions. The infringement monitoring is based on Regulation (ECB/2022/31) of the European Central Bank. The system monitors the submission of data in accordance with the reporting calendar and the fulfilment of minimum standards for accuracy and conceptual compliance. If a reporter of payment and fraud data fails to comply with the reporting requirements, the Bank of Finland will send a notification letter to the payment service provider, and the ECB may impose a fine for repeated non-compliance. The reporting of payment and fraud data will be subject to infringement monitoring as of March 2024.



2 GENERAL INSTRUCTIONS

This section describes the general principles and terms used in MAPE reporting.

In addition to the reporting instructions, the reporting is supported by the MAPE validation rules document (previously named as record structure) and code lists, which have been published on the Bank of Finland's website at: <https://www.suomenpankki.fi/en/statistics/to-the-reporter/payment-and-fraud-data/>

The website also includes links to ECB documentation where some of the requirements and instructions of the data collection are derived from.

2.1 Data to be reported

The MAPE data collection is used to collect data on payment transactions, cards, accounts and terminals, among other things. The data are related to retail payments, as opposed to wholesale payments. Retail payments refer to payments where either the payer or payee is a non-MFI (for example, a household, non-financial corporation or public corporation). In contrast, wholesale payments are payments where the payer and payee are MFIs. Data pertaining to wholesale payments are not reported in the MAPE data collection.

In payment statistics, all PSPs, also including all MAPE reporters, are included in *monetary financial institutions* (MFI). Non-MFIs (in other words, the *public*) refers to natural or legal persons which are not payment service providers.

The data are collected on an aggregated basis by attribute combinations, i.e. not as individual transactions.

2.2 Payment transactions

Payment transactions are reported in the MAPE data collection in three different record sections: HPAY, QPAY and APAY. Full reporters report the HPAY and QPAY record sections, while tail reporters report the APAY record section. The number of fields and the code values used in the fields vary. The validation rules document provides an overall view of the fields used in each payment transaction record, their code values and mandatory rules. These instructions contain a separate section for each record section with explanations of key items within the record sections.

The record sections concerning payment transactions are used to report all retail payments (*customer payments*), i.e. payment transactions initiated by non-MFIs to any counterparty and payment transactions initiated by PSPs, where the counterparty is a non-MFI.

In payment statistics, all PSPs, also including all MAPE reporters, are included in *monetary financial institutions* (MFI). Non-MFIs (also *the public*) refers to natural or legal persons which are not payment service providers.



Reportable payment transactions include:

- a) payment transactions which take place between two accounts held at different PSPs and which are executed with the use of an intermediary, i.e. where payments are sent to another PSP or to a payment system; and
- b) payment transactions which take place between two accounts held at the same PSP, e.g. “on-us transactions”, with the transaction being settled either on the accounts of the PSP itself, or with the use of an intermediary, i.e. another PSP or a payment system.

Exceptions:

- To avoid double reporting, credit transfers related to the execution of card payments and direct debits are not reported as separate transactions. This applies to both settlements related to card payments and direct debits between PSPs and settlements/deductions from a PSP to a payee.
- To avoid double reporting, payment institutions do not report the crediting of two-phase payment services from client fund accounts to payees (merchant or personal customer); in a two-phase payment service, only the first phase (so-called funding transaction) is reported in the role of payment intermediary.¹

Payment transactions initiated by a resident PSP and executed with a specific transaction order, i.e. with the use of a payment instrument, are reported broken down by the payment service used and the processing arrangement for the transaction, i.e. scheme. Payment transactions initiated by a resident PSP and executed without a specific transaction order, i.e. without the use of a payment service listed in Annex I to the Payment Services Directive, by simple book entry on the account of a non-MFI, are reported either under account “Credits to the accounts by simple book entry” or “Debits from the accounts by simple book entry”.

Fund transfers between accounts in the same name, and also between different types of accounts are included according to the payment service used. Transfers between different types of accounts include, for example, transfers from a transferable deposit to an account holding a non-transferable deposit.

In relation to bulk payment transactions, each individual payment transaction is counted.

¹ In this context, a two-phase payment service refers to different payment services where payment consists of two separate transactions: in the first one (so-called funding transaction), the funds are transferred from the payer to a client fund account held by the payment institution, and in the second phase, the funds are transferred from the payment institution’s client fund account to the actual payee.



Reportable payment transactions relate to payment transactions accumulated throughout the period, i.e. total for the reference period. The indicators on the value of transactions are compiled in euro and relate to payment transactions denominated in all currencies. Transactions denominated in foreign currency are converted into euro using the ECB reference exchange rate or exchange rates applied for these transactions.

2.3 Payment service provider's role

In the MAPE data collection, the data to be reported for each PSP depends on the payment services provided by the reporter, and the *role* of the reporter in processing payment transactions.

The processing of payment transactions is a process chain typically beginning with the initiation of a payment transaction and ending with the transfer of funds on the payee's account. The main parties to retail payments are payment service providers, payers and payees. PSPs are banks and other payment intermediaries whose services enable the transfer of money from a payer to a payee. The processing of each payment transaction may involve several PSPs in different roles. In role-specific reporting, only information relevant for each role is collected, and it is made sure that the statistics compiled includes each transaction only once (the avoidance of double reporting is also discussed in section 2.2).

PSP roles relevant for the MAPE data collection are the following.

Payer's PSP in general refers to the sender of funds. Payer's PSP usually means the PSP servicing the payer's account, or in the case of card payments, the issuer of the card. Issuer is a payment service provider referred in Article 2(2) of Regulation (EU) 2015/751 providing the payer with an instrument to make card-based payments with. The payment cards may be either physical or virtual.

Payee's PSP in general refers to the recipient of funds. Payee's PSP usually means the PSP servicing the payee's account, or in the case of card payments, the acquirer of payment transactions. The acquirer is an acquirer as defined in Article 2(1) of Regulation (EU) 2015/751 (2)(1) contracting with a payee to accept and process card-based payment transactions. In payment statistics, acquirer refers to the PSP that has a bilateral agreement with the payee, most often a merchant (end acquirer). This means that payment processors (intermediate acquirers) which do not have an agreement with the payee but function as routers towards card issuers and card schemes are not included in acquirers. Data on transactions processed by payment processors are collected in specific sections under their respective role.

Payment Initiation Service Provider (PISP) in general refers to a payment initiation service provider as defined in Article 4(18) of the Payment Services Directive. This entity provides a payment service where a user may initiate a payment order with respect to a payment account held at another payment service provider.



Account information service provider (AISP) refers to an online service as defined in Article 4(16) of the Payment Services Directive to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.

Payment intermediary (usually a payment institution) refers to payment service providers that provide services for payment intermediation but do not operate in a payment transaction as the payer's PSP (payer's account servicer or card issuer) or payee's PSP (payee's account servicer or transaction acquirer). Payment intermediaries are, for example e-commerce PSPs that provide merchants with a service to receive different payment transactions in e-commerce or within a mobile application and/or operate as mobile payment service providers, which provide a mobile payment service for the transfer of funds. These services include various digital wallets and other mobile payment solutions enabling person-to-person (P2P) or consumer-to-business (C2B) payments. In addition, payment intermediaries include, for example, different platform providers if they also operate as payment service providers in such services, i.e. transmit payments between customers.

Payment processor means a PSP that processes card payment transactions (is responsible for routing card transactions to card companies and/or card issuers) but does **not** have a direct contractual relationship with the payee for approving and processing card-based payment transactions (vs. acquirer of card payment transactions as discussed under Payee's PSP). Most often the payment processor may function in the payment process "between" the recipients of card payment transactions (payee's PSP) and card companies/card issuers.

In some cases, the PSP may function in several roles, for example as both the payer's PSP and payee's PSP as well as a PISP. In these cases, the payment transactions are reported separately for each role. The link of these roles with each type of payment service is described in more detail in these reporting instructions under the *Payment service (element paymentService)* subheadings of the respective sections concerning the HPAY, QPAY and APAY record sections.

2.4 Record sections to be reported

The MAPE data collection consists of the batch record (Header, technical record that begins the file) and content record sections. Reporting by full reporters consists of the batch record and six content record sections, while reporting by tail reporters consists of the batch record and four content record sections.

Each reporter reports the content record sections where their record section-specific reporting requirement is met. The reportable record section types depend on the payment services provided by the reporter and on its role in processing them.



The MAPE survey for full reporters comprises batch record and the following record sections:

Record section type	Use
ACCO	Accounts, deposits and offices
CARD	Number of cards
TERM	Number of terminals
HPAY	Payment transactions and fraudulent payment transactions
QPAY	Quarterly reporting of payment transactions
SERV	Customer services and electronic invoicing

The MAPE survey for tail reporters comprises batch record and the following record sections:

Record section type	Use
ACCO	Accounts, deposits and offices
CARD	Number of cards
TERM	Number of terminals
APAY	Annual reporting of payment transactions and fraudulent payment transactions

The ACCO record section is used to report data concerning the number of customer accounts, deposits and offices, among other things. The data are concerned with the amounts of the last banking day of the period under review or cumulative transactions for the period, depending on the type of data.

The CARD record section is used to report data concerning the number of cards issued, broken down by function. The data are concerned with the amounts of the last banking day of the period under review.

The TERM record section is used to report data concerning the number of terminals accepting payment instruments, broken down by function. The data are concerned with the amounts of the last banking day of the period under review.

The HPAY record section is used by full reporters to report the number and value of payment transactions and fraudulent payment transactions as well as losses due to fraud on a half-yearly basis, broken down among other things by payment service used, scheme, type of payment service user, terminal, initiation channel, strong customer authentication, fraud type, country of location of counterparty's PSP and country of location of terminal. The data are concerned with cumulative flows for the review period.

The QPAY record section is used by full reporters to report quarterly payment transactions by payment service. Card payments are reported at a more detailed level than other payment transactions. The data are concerned with cumulative flows for the review period.

The APAY record section is used by tail reporters to report the number and value of payment transactions and fraudulent payment transactions as well as losses due to fraud on an annual basis. Although the data are submitted once



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

a year, they must, however, be reported on a half-yearly basis. The data are concerned with cumulative flows for the period.

The SERV record section is used by credit institutions included in tail reporters to report data concerning customer services and invoicing. The data are concerned with the amounts of the last banking day of the period under review or cumulative transactions for the period, depending on the type of data.

2.5 Schedule of submission of fraud and payment data to Bank of Finland

Full reporters submit data to the Bank of Finland in quarterly and half-yearly intervals. Tail reporters submit the data once a year but at a half-yearly level. Tail reporters may also choose to submit the data on a half-yearly basis.

The schedules of submission of the data to the Bank of Finland are as follows:

Reporting entities	Frequency	Reference period	Submission deadline
Full reporter	Quarterly (Q)	Quarter (Q)	1 month from reference period
Full reporter	Half-yearly (H)	Half-year (H)	2 months from reference period
Tail reporter	Annually (A)	Half-year (H)	2 months (and 8 months) from reference period

The Bank of Finland announces the submission schedules of the following year's reports on its website.

2.6 Reporter's obligation to retain reported data

Reporters are obliged to retain reports submitted for the Bank of Finland's MAPE data collection for five (5) years. This obligation refers to XML-formatted report files and previously submitted CSV-formatted report files.

In developing their internal reporting systems, reporters should consider the possibility to create reports retrospectively for the purpose of revising previously submitted data. The need to submit revision reports may concern the most recent reporting periods, but the Bank of Finland may also request revisions from a longer period in case of systematic and substantial errors.



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

3 ACCOUNTS, DEPOSITS AND OFFICES (ACCO RECORD SECTION)

The ACCO record section is used to report data related to payment accounts, deposits, client funds, e-money issued and offices. The data in the ACCO record section are reported by credit institutions, payment institutions and payment service providers operating without authorisation. In other words, both full and tail reporters are obliged to report the data in the ACCO record section. As an exception, the *number of agents* is only reported by payment institutions and registered PSPs operating without an authorisation.

The data are reported with a half-yearly breakdown. Both stock and flow data are reported in the ACCO record section. Stock data refer to end-of-period, i.e. position on the last working day of the reference year-half. Flow data are concerned with cumulative data over the reporting period.

The record section includes requirements from Table 1 of the Regulation (*Institutions providing payment services to non-payment institutions*), from the Guidelines as well as national requirements.

3.1 Accounts, deposits and offices (element accounts DepositsAndOffices)

The reportable data is specified in the field (code list 1: accounts, deposits and offices) The reportable categories are as follows:

- Deposits (A010)
- Payment accounts (A020)
- Payment accounts accessed by AISPs (A021)
- Opened payment accounts with basic features (A022)
- Refused applications for payment accounts with basic features (A023)
- Switched consumers' payment accounts (A024)
- Refused applications for switching consumers' payment accounts (A025)
- Client funds (A030)
- E-money issued (A031)
- Number of AISP's clients (A040)
- Number of offices (A050)
- Number of offices offering payment services (A051)
- Number of offices offering cash services (A052)
- Number of agents (A060)

Items A010, A020, A030, A031, A050, A051, A052 and A060 are stock data, i.e. they are concerned with the situation at the end of the reporting period (last banking day of the year-half). In contrast, items A021, A022, A023, A024 and A025 are flow data, i.e. data accumulated during the reporting period.

Deposits (A010) comprise deposits from the public held by the reporting credit institution on the last banking day of the reporting period. This includes transferable overnight deposits, non-transferable overnight deposits as well



as non-overnight deposits. Deposit types are described in more detail in section [3.2](#). Only deposit accounts with a positive balance are considered deposits. Hence, the number of deposits shall not include accounts with a zero or negative balance.

Payment accounts (A020) comprises payment accounts under Article 4 of the Payment Services Directive used to execute payment transactions. Payment accounts include transferable overnight deposits (see section [3.2](#)), e-money accounts and, for example, credit card accounts with a credit feature. E-money account refers to an account in which e-money is stored and in which the balance can be used by the account holder to make payments and to transfer funds between accounts. Electronic money accounts do not include cards on which electronic money can be stored directly. All payment accounts are reported, regardless of whether the balance on the account is positive, zero or negative. Reportable number means the number of accounts at the end of the reporting period.

Payment accounts accessed by AISPs (A021) is the number of payment accounts accessed by account information service providers (AISP) during the reporting period. This data is reported by payer's PSPs, i.e. the account servicing PSP, not the AISP. Each account is reported only once even if it has been accessed multiple times. If several AISPs have accessed an account, the location (the residency) of the AISP which has accessed the account the most is reported. In case two (or more) AISPs have accessed a certain account an equal number of times during the period, report the country of the AISP which last accessed the account.

Opened payment accounts with basic features (A022) refers to payment accounts with basic features opened in the credit institution during the reporting period. Payment accounts with basic features refer to accounts defined in chapter 15, sections 6 and 6 a of the Act on Credit Institutions (610/2014), subject to the special termination and cancellation terms determined in section 6 b of said Act.

Refused applications for payment accounts with basic features (A023) refers to applications for payment accounts with basic features refused during the credit institution during the reporting period. Payment accounts with basic features refer to accounts defined in chapter 15, sections 6 and 6 a of the Act on Credit Institutions (610/2014).

Switched consumers' payment accounts (A024) comprises the number of consumers' payment accounts transferred in the switching service referred to in chapter 15 a of the Act on Credit Institutions (610/2014) during the reporting period. In accordance with section 9a of the Payment Institutions Act (297/2010/), an institution that offers payment accounts has to offer an account switching service to consumers and report to FIN-FSA thereof in line with chapter 15 a sections 2–7 of the Credit institutions Act. Only the transferring payment service provider (the PSP in which the account was held) reports this data. In this context, a consumer payment account means a payment account held in the name of one or more consumers (any natural person



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

who is primarily acting for purposes which are outside his trade, business, craft or profession) and specified in Directive 2014/92/EU (incl. Articles 1, 2 and 9).

Refused applications for switching consumers' payment accounts

(A025) comprises the number of applications for switching consumers' payment accounts refused in the switching service referred to in chapter 15 a of the Act on Credit Institutions (610/2014) during the reporting period. In accordance with section 9a of the Payment Institutions Act (297/2010/), an institution that offers payment accounts has to offer an account switching service to consumers and report to FIN-FSA thereof in line with chapter 15a sections 2–7 of the Credit Institutions Act. Only the transferring service provider reports this data. In this context, a consumer payment account means a payment account held in the name of one or more consumers (any natural person who is primarily acting for purposes which are outside his trade, business, craft or profession) and specified in Directive 2014/92/EU (e.g. Articles 1, 2 and 9).

Client funds (A030) refer to funds held by the reporter belonging to another, for example the amount of e-money issued and/or the amount of funds belonging to the payment institutions customers. Credit institutions should only report e-money issued in client funds.

E-money issued (A031) comprises the value of electronic money issued by the issuer of electronic money and other institutions than the issuer – also other issuers of electronic money than the issuer concerned – at the end of the reporting period. The value of storages also includes storages on e-money cards, on which e-money can be stored directly. Electronic money issued in all currencies is reported converted into euro.

Number of AISP's clients (A040) refers to the number clients of the Account Information Service Provider on the last day of the reference period regardless of whether the clients have used the service. This data is reported by AISPs (incl. credit institutions operating as AISPs).

Number of offices (A050) includes all offices located in the reporting country. The number of offices includes the head office but not foreign branches. The number of offices is counted as at the end of the reference period.

Number of offices offering payment services (A051) includes the number of offices includes all offices where it is possible to make payment-services related transactions, as defined in Guideline (ECB/2021/13) of the European Central Bank, annex (Table A). Payment-services-related transactions refer to transactions where a service provider acting between the payer and payee transfers funds between the parties based on an order received from them, or where a customer wishes to move money between its own payment accounts. Head offices are included in the count where it is possible to execute payment services-related transactions in the head office. These offices are also included in the item *Number of offices (A050)*



Number of offices offering cash services (A052) includes offices providing cash services. These offices are also included in the items *Offices offering payment services (A051)* and *Number of offices (A050)*. This item, similarly to the abovementioned items concerning offices, also include such PSP locations which are not necessarily traditional bank branches but where one can make cash withdrawals and deposits, for instance. Excludes bureaux de change.

Number of agents (A060) refers to agents as referred to in section 24 of the Payment Institutions Act (297/2010), through which the payment institution offers its payment services. The agent operates on behalf and at the responsibility of the payment institution. The item is only reported by payment institutions and registered PSPs.

3.2 Deposit type (element depositType)

Deposits (element accountsDepositsAndOffices, code value A010) are broken down based on the type of deposit (code list 2: deposit type). The reportable categories are as follows:

- Transferable overnight deposit (OD1)
- Non-transferable overnight deposit (OD2)
- Deposit other than an overnight deposit (NOD)

Only deposit accounts with a positive balance are considered deposits in each category. Hence, the number of deposits shall not include accounts with a zero or negative balance.

Transferable overnight deposit (OD1) refers to deposits repayable on demand and directly transferable on demand to perform a payment to a different economic agent by commonly used means of payment, such as credit transfer, direct debit, payment card or similar means, without significant delay, restriction or penalty. Accounts whose deposits may only be used for cash withdrawals and/or withdrawn or transferred only through the same account holder's other account are not transferable overnight deposit accounts.

Non-transferable overnight deposit (OD2) refers, for example, to such deposits repayable on demand which may only be used for cash withdrawals and/or withdrawn or transferred only through the same account holder's other account.

Non-overnight deposit (NOD) includes all other forms of deposit not repayable on demand, i.e. it is a residual category. This includes, for example, deposits with an agreed maturity that have an agreed fixed maturity and that cannot be converted into currency before an agreed fixed term or that can only be converted into currency before that agreed term provided that the holder is charged some kind of penalty. The category also includes so-called deposits redeemable at notice, which do not have an agreed maturity but have a notice period, during which conversion into currency is impossible or possible only with a penalty. The category also includes savings deposits or yield deposits that are in principle legally repayable on demand, but are



subject to penalties and restrictions such as restrictive drawing provisions, according to national practice. ASP deposits (deposits under the Act on Bonus for Home Savers) are classified as deposits with an agreed maturity and are therefore included in this category.

3.3 Assets transferable via network (element assetsTransferableViaNetwork)

Deposits (element accountsDepositsAndOffices, code value A010) are broken down based on whether the funds are accessible online (*true*) or not (*false*). Report the value *true* in the field for deposits which are usable electronically via the Internet or PC banking using dedicated software and dedicated telecommunication lines in order to effectuate payments. The item does not include deposits with telephone or mobile phone banking access, unless they are also accessible via the Internet or PC banking. Assets transferable via network also includes assets that can be accessed via a terminal supplied by a payment service provider. Such terminals may include ATMs with additional functionality or other devices supplied by the PSP which are connected to the account via telecommunication. As regards deposits other than those transferable via telecommunication, report the value *false*.

3.4 E-money account (element eMoneyAccount)

Payment accounts (element accountsDepositsAndOffices, code value A020) are broken down based on whether they are e-money accounts (*true*) or not (*false*). Report the value *true* in the field, if the account is an e-money account. E-money account refers to an account in which e-money is stored and

Definition of electronic money as per Directive 2009/110/EC, Article 2(2):

Electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in Article 4(5) of Directive (EU) 2015/2366, and which is accepted by a natural or legal person other than the electronic money issuer.

Directive 2009/110/EC should not apply to monetary value stored on specific pre-paid instruments, designed to address precise needs that can be used only in a limited way, because they allow the electronic money holder to purchase goods or services only in the premises of the electronic money issuer or within a limited network of service providers under direct commercial agreement with a professional issuer, or because they can be used only to acquire a limited range of goods or services.

Instruments which can be used for purchases in stores of listed merchants should not be exempted from the scope of this Directive as such instruments are typically designed for a network of service providers which is continuously growing.

It is also appropriate that this Directive not apply to monetary value that is used to purchase digital goods or services, where, by virtue of the nature of the good or service, the operator adds intrinsic value to it, e.g. in the form of access, search or distribution facilities, provided that the good or service in question can be used only through a digital device, such as a mobile phone or a computer, and provided that the telecommunication, digital or information technology operator does not act only as an intermediary between the payment service user and the supplier of the goods and services. This is a situation where a mobile phone or other digital network subscriber pays the network operator directly and there is neither a direct payment relationship nor a direct debtor-creditor relationship between the network subscriber and any third-party supplier of goods or services delivered as part of the transaction.



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

in which the balance can be used by the account holder to make payments and to transfer funds between accounts. Electronic money accounts do not include cards on which electronic money can be stored directly. In case of non-e-money payment accounts, report the value *false* in the field.

3.5 Payment service user (element `paymentServiceUser`)

Deposits (element `accountsDepositsAndOffices`, code value A010) and payment accounts (element `accountsDepositsAndOffices`, code value A020) are broken down based on the user of the payment service, i.e. customer type (code list 3: payment service user type). The reportable categories are as follows:

- Personal customer (P)
- Corporate customer (C)

The breakdown into personal and corporate customers is made based on business ID.

Personal customer (P) is a payment service user not operating under a business ID. This item also includes, for example, sole proprietors not operating under a business ID.

Corporate customer (C) is a payment service user operating under a business ID. This item also includes, for example, public corporations operating under a business ID.

3.6 Country (element `country`)

Payment accounts accessed by AISPs (element `accountsDepositsAndOffices`, code value A021) and number of AISP's clients (element `accountsDepositsAndOffices`, code value A040) are reported by country, using the values in the code list *Country* (ISO 3166). In the case of payment accounts, country refers to the country of location of the AISP, and in the case of AISP's clients, it refers to the residency of the clients.



4 NUMBER OF CARDS (CARD RECORD SECTION)

The CARD record section is used to report cards issued by the PSP, broken down by function. The data are reported by both full and tail reporters. The data are reported by card issuers. The card issuer reports the data regardless of the cardholder's residency or the location of the account to which the card is linked. The cardholder's residency is reported in country element (*Country*) of the CARD record section.

The data in the CARD record section are reported using a half-yearly breakdown. The data reported in the CARD record section are stock data referring to end-of-period, i.e. positions on the last banking day of the reference year-half.

The number of cards is reported based on card number, i.e. PAN number (primary account number), as opposed to the number of physical cards, i.e. "plastic cards". For example, combination cards including both a debit function and a credit function are counted as two separate cards. Cards in circulation are included irrespective of when they were issued or whether they were used. Expired or withdrawn cards are not included. The number of cards is reported regardless of when they have been issued or whether they have been used. Expired or withdrawn cards are excluded.

Only general-purpose cards are reported, meaning that cards with a restricted purpose of use are not reported. Cards issued by merchants, i.e. retailer cards, are not included, unless they have been issued in cooperation with a PSP, i.e. they are co-branded. Also, cards issued by card schemes, i.e. three-party or four-party schemes, are included.

The record section corresponds to the requirements of Table 2 (*Card functions*).

4.1 Card type (element cardType)

Cards are reported based on card type (code list 4: card type). The reportable card type categories are as follows:

- Debit card
 - Online debit card (C111)
 - Offline debit card (C112)
- Delayed debit card (C120)
- Credit card (C130)
- E-money card (C200)
- Card other than a payment card (C900)

Debit card is a card enabling cardholders to have their purchases directly and immediately charged to their bank accounts. A card with a debit function may be linked to an account offering overdraft facilities as an additional feature. The number of cards with a debit function refers to the total number of cards (PAN numbers) in circulation and not to the number of accounts to which the cards are linked. The distinguishing feature of a card with a debit



function, in contrast to a card with a credit function or a delayed debit function, is the contractual agreement to charge purchases directly to the bank account linked to the card. The total number of cards with a debit function is not reported, since debit cards are broken down into online debit and offline debit cards.

Online debit card (C111) is a card requiring electronic preauthorisation of funds on the payment account. The payment is immediately deducted from the available account balance.

Offline debit card (C112) is a card on which funds are not always preauthorised when a purchase takes place.

Delayed debit card (C120) is a card enabling the cardholder to have purchases (incl. cash withdrawals) charged to an account with the card issuer, up to an authorised limit. The balance in this account is then settled in full at the end of a pre-defined period. The distinguishing feature of a card with a delayed debit function, in contrast to a card with a credit function or a debit function, is the contractual agreement granting a credit line but with an obligation to settle the debt incurred at the end of a pre-defined period. If the card has a credit function, it is not reported here but in category C130, credit card. A delayed debit card is reported as a credit card if the delayed debit function cannot be specified. The same logic applies to the reporting of transactions made with a delayed debit card.

Credit card (C130) is a card enabling the cardholder to make purchases, and in some cases also to withdraw cash, up to a pre-arranged ceiling. The credit granted may be settled in full by the end of a specified period or may be settled in part, with the balance taken as extended credit on which interest is usually charged. The distinguishing feature of a card with a credit function, in contrast to a card with a debit function or a delayed debit function, is the contractual agreement granting the cardholder a credit line allowing for extended credit.

E-money card (C200) is a card enabling e-money payment transactions. This includes cards on which e-money can be stored directly and/or cards which give access to e-money stored on e-money accounts. Electronic money (e-money) means 'electronic money' as defined in Article 2(2) of Directive 2009/110/EC (see definition in section 3.4).

(Gift) vouchers accepted by a limited number of merchants are not included in e-money cards on which electronic money can be deposited directly. Monetary value stored on specific prepaid instruments does not represent electronic money if the instruments can be used only in a limited range of products or services. Such instruments may include store cards, petrol cards, membership cards, public transport cards, meal vouchers or vouchers for services. These cards and transactions with these cards are not included in the reporting of payments statistics.



Card other than a payment card (C900) is a card that does not belong to the other categories. It may be, for example, a cash card enabling the holder to withdraw cash from an ATM and/or to deposit cash to an ATM.

4.2 E-money card type (element eMoneyCardType)

The type of e-money card is only reported for e-money cards (C200). E-money cards are reported based on the type of e-money card (code list 5: e-money type). The reportable categories are as follows:

- Cards on which e-money can be stored directly
 - Cards on which e-money can be stored directly (activated) (E11)
 - Cards on which e-money can be stored directly (not activated) (E12)
- Cards linked to an e-money account (E21)

Card on which e-money can be stored directly is an e-money card which is not linked to an e-money account, but electronic money is only directly stored on the card. The total number of cards is not reported, but activated and not activated cards are reported separately.

Card on which e-money can be stored directly (activated) (E11) is a card not linked to an e-money account, on which e-money has been loaded at least once. Loading may be interpreted as indicative of the intention to use the e-money function. The time of loading is irrelevant, i.e. it may have occurred outside the reporting period. Only cards valid at the end of the reporting period are included.

Card on which e-money can be stored directly (not activated) (E12) is a card not linked to an e-money account, on which e-money has never been loaded.

Card linked to an e-money account (E21), is an e-money card enabling the use of electronic money (see the definition of electronic money in [section 3.4](#)). This does not include cards on which electronic money can be deposited directly.

4.3 Scheme (element scheme)

Cards are reported according to the payment scheme (code list 6: scheme). The reportable categories are as follows:

- Visa (VISA)
- MasterCard (MCRD)
- American Express (AMEX)
- Diners Club (DINE)
- Other (OTH)

Visa (VISA) comprises cards that belong in terms of technical and commercial arrangements to the VISA product family (e.g. VISA Credit, Visa Electron, VPAY).



Mastercard (MCRD) comprises cards that belong in terms of technical and commercial arrangements to the Mastercard product family (e.g. Mastercard, Maestro).

American Express (AMEX) comprises cards that belong in terms of technical and commercial arrangements to the American Express product family.

Diners Club (DINE) comprises cards that belong in terms of technical and commercial arrangements to the Diners Club product family.

Other (OTH) comprises cards functioning with other arrangements.

4.4 Cash function (element cashFunction)

The field is reported as *true* for cards enabling the holder to withdraw cash from an ATM and/or to deposit cash to an ATM. In addition to the cash function, the card may also have other functions. If the card does not have a cash function, report *false*.

4.5 Combination card (element combinationCard)

Cards are broken down based on whether they are combination cards or not (code list 7: combination card). The reportable categories are as follows:

- Non-combination card (NC)
- Combination card (CC)
- Combination card with an e-money function (EC)

Non-combination card (NC) includes cards that only have a cash payment, delayed debit and/or credit or e-money function, but not a combination of these.

Combination card (CC) includes cards that offer a debit function combined with a delayed debit function or a debit function combined with a credit function. The category contains typical combination cards used in Finland.

E-money combination card (EC) comprises cards with a combined cash, debit and e-money function.

4.6 Card technology (element cardTechnology)

Cards are reported according to the card technology (code list 8: card technology). The reportable categories are as follows:

- Chip card with an NFC (Near Field Communication) function (C1)
- Chip card without an NFC function (C2)
- Magnetic stripe card (M)
- Virtual card (V)

Chip card with an NFC function (C1) is a chip card that allows a card payment transaction to be initiated with a particular type of contactless



technology and where both the payer and the payee of the payment transaction (and/or their equipment) are in the same physical location.

Chip card without an NFC function (C2) comprises chip cards that do not have an NFC function.

Magnetic stripe card (M) covers cards that only have a magnetic stripe.

Virtual card (V) is a card that only exists in a virtual form (no physical plastic card). E-money cards that only exist in a virtual form are also included. Cards with both a physical and digital form are excluded from this category, as they are included in some of the other categories in this field depending on the features of the physical card.

4.7 Payment service user (element paymentServiceUser)

Cards are reported based on their user (code list 3: type of payment service user). The reportable categories are as follows:

- Personal customer (P)
- Corporate customer (C)

Personal customer (P) is a payment service user not operating under a business ID. This item also includes, for example, sole proprietors not operating under a business ID

Corporate customer (C) is a payment service user operating under a business ID. This item also includes for example, public corporations, operating under a business ID.

4.8 Country (element country)

The country code reported in the CARD record section refers to the cardholder's residency. The country is reported using the code values in code list *Country (ISO 3166)*.



5 NUMBER OF TERMINALS (TERM RECORD SECTION)

The TERM record section is used to report the number of terminals by function. The data in the record section are reported by credit institutions, payment institutions and payment service providers operating without authorisation. In other words, both full and tail reporters are obliged to report the data in the TERM record section. The data in the record section are reported on a half-yearly basis. The data reported in the TERM record section are stock data referring to end-of-period, i.e. positions on the last banking day of the reference year-half.

The number of terminals is reported by the acquirers. Acquirer is the operator that has a direct contractual relationship with the customer (merchant) for crediting payment transactions, as described in section 2.1.

The reporters should report all physical devices and terminals at which transactions are acquired by them, also including terminals located outside of the reporting country. Every terminal is counted individually even if several terminals of the same type exist at one merchant location

The record section corresponds to the requirements of Table 3 (*Card accepting devices*).

5.1 Terminal type (element terminalType)

Terminals are reported based on their type (code list 9: type of terminal). The reportable categories are as follows:

- Physical POS (T011)
- Credit transfer ATM (TO22)

Physical POS (T011) is a point-of-sale device allowing the use of payment cards at a physical (not virtual) point of sale. The payment information is captured either manually on paper vouchers or by electronic means, i.e. EFTPOS. This also includes terminals allowing the transfer of electronic value from an issuer of electronic money to a card with an e-money function and vice versa or from the balance on the card to the balance of a beneficiary. In addition, the category includes terminals with a dual functionality, i.e. which function both as EFTPOS and e-money terminals, as well as terminals with an e-money function only.

Credit transfer ATM (TO22) is an ATM allowing authorised users to make credit transfers using a payment card.

5.2 EFTPOS (element eftpos)

Report *true* in the field if the terminal concerned is an EFTPOS. EFTPOS terminals are terminals of an electronic direct-debit system which receive payment data electronically. The terminals have been designed, in some cases, to transmit such information either online, with a real-time request for



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

authorisation, or offline. This also includes unattended terminals. If the terminal is not an EFTPOS, report *false*.

5.3 Contactless payment (element `contactlessPayment`)

Report *true* in the field, if the payment terminal concerned supports contactless communication payments. Otherwise, report *false*.

5.4 Terminal accepting e-money (element `terminalAcceptingEMoney`)

Report *true* in the field in case of terminals allowing holders of e-money on a card with an e-money function to transfer e-money value from their balance to the balance of a merchant or other beneficiary. If the terminal is not an e-money accepting terminal, report *false*.

5.5 E-money loading/unloading (element `eMoneyLoadingUnloading`)

Report *true* in the field in case of terminals allowing the transfer of electronic value from an issuer of electronic money to the holder of a card with an e-money function and vice versa, i.e. loading and unloading. If the terminal is not suitable for loading or unloading electronic money, report *false*.

5.6 Country (element `country`)

The country reported in the field refers to the country of location of the terminal. The country is reported using the code values in code list *Country (ISO 3166)*.



6 ANNUAL REPORTING OF PAYMENT TRANSACTIONS AND FRAUDULENT PAYMENT TRANSACTIONS (APAY RECORD SECTION)

In the APAY record section, tail reporters report half-yearly data on payment transactions, fraudulent payment transactions and losses due to fraud.

General instructions on the reporting of payment transactions and the roles of the reporters are available in section 2 of these instructions.

6.1 Reporter's role (element reportersRole)

For payment transactions, the role of the payment service provider (PSP) is reported (code list 12: payment service provider's role). The reportable roles are as follows:

- Payer's PSP (ER)
- Payee's PSP (EE)
- PISP (PI)
- Payment intermediary (IM)
- Payment processor (PO)

The payment service provider's role refers to the capacity in which the PSP is involved in the payment transaction: the payer's PSP, the payee's PSP, the payment service provider, payment intermediary or payment processor.

Payer's PSP (ER), or the payer's payment service provider, means the sender of the funds. Payer's PSP usually means the PSP servicing the payer's account, or in the case of card payments, the issuer of the card. Issuer is a payment service provider referred to in Article 2(2) of Regulation (EU) 2015/751 providing the payer with an instrument to make card-based payments with. The payment cards may be either physical or virtual.

Payee's PSP (EE), or the payee's payment service provider, means the recipient of the funds. Payee's PSP usually means the PSP servicing the payee's account, or in the case of card payments, the acquirer of payment transactions. The acquirer is an acquirer as defined in Article 2(1) of Regulation (EU) 2015/751 (2)(1) contracting with a payee to accept and process card-based payment transactions. In payment statistics, acquirer refers to the PSP that has a bilateral agreement with the payee, most often a merchant (end acquirer). This means that payment processors (intermediate acquirers) which do not have an agreement with the payee but function as routers towards card issuers and card schemes are not included in acquirers. Data on transactions processed by payment processors are collected in specific sections under their respective role.

Payment Initiation Service Provider (PI, PISP) refers to a service provider as defined in Article 4(18) of the Payment Services Directive. If the reporting PSP provides payment initiation services, said provider must report, in the role of PISP, any payments initiated by it on behalf of customers (its own and others' customers), i.e. credit transfers and other payments initiated by the PISP itself. Credit transfers and other payments reported as PISP do not



contribute to the total number, or total value of credit transfers reported as payer's PSP. If a reporter has a double role, for example as payers' PSP and PISP, it must report payments made in each of the roles separately.

Payment intermediary (IM) (usually a payment institution) refers to payment service providers that provide services for payment intermediation but do not operate in a payment transaction as the payer's PSP (payer's account servicer or card issuer) or the payee's PSP (payee's account servicer or transaction acquirer). Payment intermediaries are, for example PSPs that

- operate as e-commerce merchant/PSPs i.e. providing merchants with a service to receive different payment transactions in e-commerce or within a mobile application
- operate as mobile payment service providers, which provide a mobile payment service for the transfer of funds. These services include various digital wallets and other mobile payment solutions enabling person-to-person (P2P) or consumer-to-business (C2B) payments and/or
- are platform providers where the platform provider also operates as a PSP transmitting payments between customers.

Payment processor (PO) is the role used to report card payments where the PSP operates as a processor of card payments (responsible for routing to card schemes and card issuers) but where the PSP does not have a direct agreement with the payee (merchant or private customer) for accepting and processing card-based payment transactions. Most often the payment processor may function in the payment process "between" the recipients of card payment transactions (payee's PSP) and card companies/card issuers.

If the reporter operates in more than one reportable role in a payment transaction, the payment transaction must be reported separately for each role.

6.2 Information type (element informationType)

Different types of information are reported on payment transactions (code list 10: information type). The reportable types are as follows:

- Payment transaction (PT)
- Fraudulent payment transaction (FT)
- Losses due to fraud (LF)

Payment transaction (PT) is an operation where funds are used, transferred, deposited or withdrawn. In reportable payment transactions, at least one of the parties involved is a non-MFI. Also includes fraudulent payment transactions.

Fraudulent payment transaction (FT) includes unauthorised payment transactions. These include for example transactions resulting from the loss, theft or misappropriation of sensitive payment data or a payment instrument,



whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer. In addition, the category includes payment transactions where the fraudster has manipulated the payer to initiate the payment transaction. Cases where the payee is fraudulent, for example selling a non-existent/counterfeit product or service, but the fraud is not directly involved with the payment process are excluded from fraudulent transactions.

Fraudulent payment transactions are reported based on the date when the fraud was discovered. Payment service providers should report all fraudulent payment transactions as from the moment when the fraud is detected through a complaint by a client or other means, regardless of whether the incident related to the fraudulent payment transactions has been investigated by the time of reporting.

Losses due to fraud (LF) refers to the losses by the reporting payment service provider, its payment service user or others, reflecting the actual impact of fraud on a cash flow basis. Since the registering of financial losses borne may be disassociated time-wise from the actual fraudulent transactions and in order to avoid revisions of reported data purely due to this immanent time lag, the final fraud losses should be reported in the period when they are recorded in the payment service provider's books. The final fraud loss figures should not take into account refunds by insurance agencies because they are not related to fraud prevention for the purposes of PSD2.

6.3 Payment service (element paymentService)

Transactions are reported based on their type (code list 11: type of payment transaction). The reportable types are as follows:

- Credit transfer (CT)
- Direct debit (DD)
- Card payment (CP)
- Cash withdrawal (CW)
- Electronic money payment (EMP)
- E-money card loading or unloading (EML)
- Cheque (CHQ)
- Money remittance (MR)
- Other payment service included the scope of the Payment Services Directive (OTD)
- Credits to the account by simple book entry (CBE)
- Debits from the account by simple book entry (DBE)
- Other payment service, not included in the Payment Services Directive (OTN)
- Refunded card payment (RCP)

Credit transfer (CT) is a payment service that allows the payer to instruct the institution holding its account to transfer funds to the beneficiary. It is a payment order or a sequence of payment orders made for the purpose of placing



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

funds at the disposal of the beneficiary. Both the payment order and the funds described therein move from the PSP of the payer to the PSP of the payee, i.e. the beneficiary, possible via several other credit institutions as intermediaries and/or one or more payment and settlement systems.

Transactions involving cash at one or both ends of the payment transaction, and utilizing a credit transfer payment service, are included as credit transfers. Credit transfers initiated at an ATM with a credit transfer function are also included. Credit transfers also comprise transfer of funds from the credit card to the account and transfer of other revolving credits to the account.

Fund transfers between accounts in the same name, and also between different types of accounts, are included. Transfers between the same owner's accounts are reported regardless of the type of account. These include, for example, transfers between current accounts and savings accounts.



Credit transfers

Example 1:

Customer's account (in Bank A) \longrightarrow Customer's account (in Bank B)

- The payment should be included in payment statistics:
 - Bank A reports a credit transfer sent from a customer's account in the role of payer's PSP (element reportersRole).
 - Bank B reports a credit transfer received on a customer's account in the role of payee's PSP (element reportersRole).
 - If Bank A and B are the same institution (both the payer and payee's accounts are in the same bank), the institution reports both transactions as described above. In this case, payments are usually categorised as on-us payments (i.e. if a payment is not sent to any payment system but is executed by internal recognitions within the bank, the reported payment scheme/payment is "on-us").

Example 2:

Payment service provider's account (in Bank A) \longrightarrow Customer's account (in Bank B)

- The payment should be included in payment statistics:
 - Bank A reports a credit transfer sent from its own account in the role of payer's PSP (element reportersRole).
 - Bank B reports a credit transfer received on a customer's account in the role of payee's PSP (element reportersRole).
 - If Bank A and B are the same institution (both the payer and payee's accounts are in the same bank), the institution reports both transactions as described above. In this case, payments are usually categorised as on-us payments (i.e. if a payment is not sent to any payment system but is executed by internal recognitions within the bank, the reported payment scheme/payment is "on-us").

Example 3:

Customer's account (in Bank A) \longrightarrow Payment service provider's account (in Bank B)

- The payment should be included in payment statistics:
 - Bank A reports a credit transfer sent from a customer's account in the role of payer's PSP (element reportersRole).
 - Bank B reports a credit transfer received on its own account in the role of payee's PSP (element reportersRole).
 - If Bank A and B are the same institution (both the payer and payee's accounts are in the same bank), the institution reports both transactions as described above. In this case, payments are usually categorised as on-us payments (i.e. if a payment is not sent to any payment system but is executed by internal recognitions within the bank, the reported payment scheme/payment is "on-us").

Example 4:

Payment service provider's account (in Bank A) \longleftrightarrow Payment service provider's account (in Bank B)

- This kind of payments are not included in payment statistics. In other words, payments where both the payer and payee are a PSP must not be included in statistical reporting. Only payments where the participant at either end is a customer should be included.

Note! Examples 2 and 3 should not be confused with credits to the account by simple book entry or debits from the account by simple book entry.



Credit transfers	
Role	More detailed description of reportable data
Payer's PSP	In credit transfers, the payer's account servicer is considered the payer's PSP. The payer's PSP reports payments initiated by its customers and the PSP itself. <ul style="list-style-type: none"> • Credit institutions report credit transfers sent even where the sender is a payment institution (or another credit institution) whose account is serviced by the credit institution.
Payee's PSP	In credit transfers, the payee's account servicer is considered the payee's PSP. The payee's PSP reports payments received by its customers and the PSP itself. <ul style="list-style-type: none"> • Credit institutions report credit transfers received even where the recipient is a payment institution (or another credit institution) whose account is serviced by the credit institution.
Payment intermediary	In credit transfers, payment intermediary means a PSP providing a payment service based on credit transfer but not operating as the payer's PSP or payee's PSP. Examples include payments initiated by the payer in e-commerce as credit transfers and using a mobile payment solution as credit transfers and payments initiated on various platform services as credit transfers. Purchases made by the payer in e-commerce using an invoice, credit or instalment solution are also reported under credit transfers.
Payment initiation service provider (PISP)	Credit transfers initiated by a PISP on behalf of its customer in the role of a PISP. Note. The PSP servicing the account where the payment is initiated using a payment initiation service reports the payments as payer's PSP – not as PISP.

Direct debit (DD) is a payment service where an invoice sender requests a PSP to debit a payer's payment account, potentially on a recurrent basis, on the basis of the payer's consent. Direct debit includes only payments under the SEPA SDD Core and SEPA SDD B2B schemes.

Direct debits are reported both by the payee's PSP and payer's PSP. The invoice senders (payee's) payment service provider reports direct debit requests sent as the payee's PSP (EE), and the payer's payment service provider reports direct debit requests received in the role of payer's PSP (ER). Both one-off and recurrent direct debits are counted. Each debit under recurrent direct debits is counted as a single transaction. Rejected direct debit requests are included in reportable direct debit. Rejected direct debit requests include all direct debit requests already initiated by the invoice sender's (payee's) PSP regardless of the phase where and reason why they are subsequently rejected. However, cancelled direct debit requests are not reported. Direct debits used to settle outstanding credit balances resulting from card payments are included as direct debits. These are separate payments from the cardholder to the card issuer.



Direct debits	
Role	More detailed description of reportable data
Payer's PSP	In direct debits, the payer's account servicer is considered the payer's PSP. Payer's PSP reports direct debit requests received <ul style="list-style-type: none"> • Credit institutions report direct debits received even where the recipient is a payment institution (or another credit institution) whose account is serviced by the credit institution.
Payee's PSP	In direct debits, the payee's (invoice sender's) account servicer is considered the payee's PSP. Payee's (invoice sender's) PSP reports direct debit requests sent <ul style="list-style-type: none"> • Credit institutions report direct debits sent even where the sender is a payment institution (or another credit institution) whose account is serviced by the credit institution.

Card payment (CP) includes payment transactions made with a payment card (excluding cards with an e-money function only). The card issuer reports card payments made both in the home country and abroad using cards issued by it. The acquirer of the card payment reports card payments received at physical and virtual POS terminals operated by it both in the home country and abroad. Payment transactions made in e-money are not included.

Card payments include payment transactions performed using cards with a debit, credit or delayed debit function at a terminal (physical or virtual) or via other channels. Payments initiated both with a physical card and a mobile solution are reported. All payment transactions initiated with a card are included, i.e.:

- (a) (all transactions in which the acquirer and the issuer of the card are different entities; and
- (b) all transactions in which the acquirer and the issuer of the card are the same entity.

Deductions from the PSP's account resulting from the settlement of a card transaction in which the acquirer and the issuer of the card are the same entity are included.

Card payments do not include cash withdrawals and deposits at ATMs. Credit transfers at ATMs are not included in card payments. Neither do card payments include cash advances and deposits at POS terminals.



Card payments (ER and EE roles)

Example 1:

A customer initiates a card payment at a physical or virtual terminal using a card.

- The card payment is included in payment statistics as follows:
 - The issuer of the card reports the card payment sent from a card issued by it in the role of payer's PSP (element reportersRole).
 - The acquirer of the card payment reports the card payment received in the role of payee's PSP (element reportersRole).
 - Note! Card payment transactions may also involve other parties (payment processors and payment intermediaries). Instructions concerning PSP's functioning in different roles in card payment transactions are found in the role-specific table below and in chapter 6.1 Reporter's role.

Example 2:

A customer initiates a card payment at a physical or virtual terminal using a mobile application. The payment transaction is executed on the card rail.

- The card payment is included in payment statistics as follows:
 - The issuer of the card reports the card payment sent from a card issued by it in the role of payer's PSP (element reportersRole).
 - The acquirer of the card payment reports the card payment received in the role of payee's PSP (element reportersRole).
 - Note! Card payment transactions may also involve other parties (payment processors and payment intermediaries). Instructions concerning PSP's functioning in different roles in card payment transactions are found in the role-specific table below and in chapter 6.1 Reporter's role.

Example 3:

A customer returns a product purchased by them to the merchant, who refunds the customer's funds to the customer's card.

- The refunded card payment is included in payment statistics as follows:
 - The initiator of the refund transaction, i.e. the merchant's PSP (acquirer), reports the card payment sent to the customer's card in the role of payer's PSP (element reportersRole).
 - The acquirer of the refund transaction, i.e. the issuer of the card, reports the card payment received on a card issued by it in the role of payee's PSP.
 - Note! Only refund transactions made on the card rail are included in refunded card payments. If the refund is made as a credit transfer, the refund transaction is reported as a credit transfer. For more information on refunded card payments, see page 41.

Example 4:

A card payment initiated by a customer is cancelled before the card payment is credited to the merchant.

- Cancelled card payments are not included in payment statistics. Cancelled card payments are deducted from the original payment transaction, and the cancellation is not reported as a separate payment transaction.



Card payments	
Role	More detailed description of reportable data
Payer's PSP	In card payments, the card issuer is considered the payer's PSP. The payer's PSP reports payments made with cards issued by it.
Payee's PSP	In card payments, the acquirer of card transactions is considered the payee's PSP. The acquirer means the PSP with a direct contract with the payee (merchant or private customer) on the acceptance and processing of card-based payment transactions (cf. payment processor). The payee's PSP, i.e. the acquirer of card payments reports card payments received.
Payment processor	In card payments, payment processor refers to a PSP involved in the transmission of card payments without a direct contract with the payee (merchant or private customer), i.e. which does not operate as an acquirer. (See the definition of <i>acquirer</i> under payee's PSP.)
Payment intermediary	In card payments, payment intermediary means a PSP providing a payment service based on card payment but not operating as the payer's PSP, payee's PSP or payment processor.

Cash withdrawals (CW) include cash transactions broken down by the manner of withdrawals into ATM cash withdrawals, cash back at POS terminals, OTC cash withdrawals and other cash withdrawals, such as cash ordered by post and corporate customers' change cash withdrawals via cash transit boxes or cash-in-transit services.

Cash withdrawals	
Cash withdrawals at ATM	
Role	More detailed description of reportable data
Payer's PSP	In ATM cash withdrawals with cards, the issuer of the card is considered the payer's PSP. The payer's PSP reports cash withdrawals made at an ATM with cards issued by it.
Cash withdrawals at retail merchants	
Role	More detailed description of reportable data
Payer's PSP	In cash withdrawals at POS, the issuer of the card is considered the payer's PSP. The payer's PSP reports cash withdrawals made at retail merchants with cards issued by it.
Non-card cash withdrawals	
Role	More detailed description of reportable data
Payer's PSP	In non-card cash withdrawals, the account servicer of the withdrawer is considered the payer's PSP. The payer's PSP reports cash withdrawals and deposits from accounts held by it that are made by other means than cards. These include OTC cash withdrawals and deposits, cash orders via post and for example corporate customers' change cash withdrawals via cash transit boxes and cash-in-transit services.



E-money payment (EMP) is a transaction whereby a holder of e-money transfers e-money value from its own balance to the balance of the beneficiary, either with a card on which e-money can be stored directly or with other e-money accounts. See also the definition of electronic money and e-money account in section 3.4.

E-money card-loading or unloading (EML) includes transactions where electronic money value is transferred from the issuer of electronic money onto a card equipped with an e-money function or vice versa. This includes both the loading and unloading of an e-money card. See also the definition of electronic money in section 3.4.

Electronic money payment	
Payments with e-money cards	
Role	More detailed description of reportable data
Payer's PSP	In payments made with e-money cards and in e-money card loading and unloading, the issuer of the e-money card is considered the payer's PSP. Payer's PSP reports payments made with e-money cards issued by it as well as e-money card loading and unloading. Both payments with cards on which e-money can be stored directly and payments with cards linked to an e-money account are reported.
Payee's PSP	In payments made with e-money cards and in e-money card loading and unloading, the acquirer of the e-money card transactions is considered the payee's PSP. Payee's PSP, i.e. the recipient of e-money card transactions, reports received payments made with e-money cards and in e-money card loading and unloading. Both payments with cards on which e-money can be stored directly and payments with cards linked to an e-money account are reported.
Payment intermediary	In e-money card payments, payment intermediary refers to a PSP providing a payment service based on e-money card payment but not operating as the payer's PSP or payee's PSP.
Other electronic money payments	
Role	More detailed description of reportable data
Payer's PSP	In other electronic money payments, the servicer of the payer's e-money account is considered the payer's PSP. The payer's PSP reports non-card payments made from e-money accounts held by it.
Payee's PSP	In other electronic money payments, the servicer of the payee's e-money account is considered the payee's PSP. The payer's PSP reports non-card payments received on e-money accounts held by it.
Payment intermediary	In other electronic money payments, credit intermediary refers to a PSP providing a payment service based on other (than card) electronic money payment but not operating as the payer's PSP or payee's PSP.



Cheque (CHQ) is a written order from one party, i.e. the drawer, to another, i.e. the drawee, normally a credit institution, requiring the drawee to pay a specified sum on demand to the drawer or to a third party specified by the drawer.

Cash withdrawals with cheques are included. Cash withdrawals using bank forms are not included. Cheques issued but not submitted for clearing are not included.

Cheques	
Role	More detailed description of reportable data
Payer's PSP	Payer's PSP reports payment instructions/cheques received
Payee's PSP	Payee's PSP reports payment instructions/cheques sent

Money remittance (MR), as defined in Article 4(22) of the Payment Services Directive, means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee. Also includes payment orders.

Money remittances	
Role	More detailed description of reportable data
Payer's PSP	Payer's PSP reports money remittances sent.
Payee's PSP	Payee's PSP reports money remittances received.

Other payment service included the scope of the Payment Services Directive (OTD) comprises other payment services falling within the scope of the Payment Services Directive (PSD2) but which cannot be reported in any other category.

Other payment service included in the Payment Services Directive	
Role	More detailed description of reportable data
Payer's PSP	Depends on the payment service
Payee's PSP	Depends on the payment service
Payment initiation service provider	Other payment services included in the Payment Services Directive initiated by a PISP on behalf of its customers in the role of a PISP.

Credit to the account by simple book entry (CBE) includes all of the following credits made by a PSP to its customers' accounts: (i) interest payments; (ii) dividend payments; (iii) disbursement of the amount of a loan to the current account of the customer; (iv) other credits to the account by simple book entry.



Credit to the account by simple book entry means an item whereby the bank automatically credits a client's account without requiring a separate payment order from the client. This data is excluded from credit transfers. Transfer of a card credit or revolving credit to the account is not a simple book entry.

Credits to the account by simple book entry	
Role	More detailed description of reportable data
Payer's PSP	The payment service provider reports credits to accounts using a simple account entry

Debit from the account by simple book entry (DBE) includes the PSP's own debits, for example debiting of loan interest: The following transactions are reported for this category: (i) charge of interest by the bank; (ii) deduction of banking fees; (iii) payment of taxes linked to financial assets, if they are a separate transaction but not separately authorised by the customer; (iv) re-payments of capital on a loan; (v) other debits to the account by simple book entry. Debit from the account by simple book entry means an item whereby the bank automatically debits a client's account without requiring a separate payment order from the client. These data are excluded from direct debits. Card related annual fees and service fees belong to this category.

Debits from the account by simple book entry	
Role	More detailed description of reportable data
Payee's PSP	The payment service provider reports debits from accounts using a simple account entry

Other payment service not included the scope of the Payment Services Directive (OTN) comprises other payment services falling outside the scope of the Payment Services Directive (PSD2) and which cannot be reported in any other category.

Other payment service, not included in the Payment Services Directive	
Role	More detailed description of reportable data
Payer's PSP	Depends on the payment service
Payee's PSP	Depends on the payment service

Refunded card transaction (RCP) includes refunds and chargebacks of card payments made on the card rail and other card payments in the opposite direction where funds are being credited to the payment card. The chargeback of a card payment is a payment transaction separate from the original card payment, which cannot be linked to the original payment transaction. An example of a chargeback is when a customer returns a previously purchased product to the store and the merchant repays the money to the customer. A reverse POS transaction is reported as the opposite of a card-based payment transaction at a POS. The transaction is reported both by the merchant's PSP (payee's PSP in the original payment transaction) and the issuer of the card. In card refunds, it is decisive that the funds are refunded to the card itself, not



a bank account. Refunds or repayments made as a credit transfer are reported as credit transfers.

Refunded card payment	
Role	More detailed description of reportable data
Payer's PSP	Initiated refunded card payments are reported by the acquirer of the original card payment, i.e. the merchant's PSP. Card payment refunds initiated in other refund transactions on the card rail are reported in the role of payer's PSP by the party initiating the refund transaction.
Payee's PSP	Received refunds of card payments are reported by the issuer of the card being credited. Card payment refunds received in other refund transactions on the card rail are reported in the role of payee's PSP by the issuer of the card being credited.

6.4 Electronic (element electronic)

Report *true* in the field if the payment order is electronic. Otherwise, report *false*.

Credit transfers are considered as electronic (*true*) if the payer submits them electronically. Credit transfers are considered as non-electronic (*false*) if they are initiated by the payer in paper-based form or by instructing staff at a branch over the counter (OTC) to initiate a credit transfer or if the credit transfer requires manual processing. Also, credit transfers which are initiated non-electronically but not in paper-based form, e.g. mail order or telephone order (MOTO) transactions, are considered as non-electronic credit transfers. In the case of recurrent payments, the value of the field is determined based on how the payment order was made, not how the payment was executed. Hence, for example if a recurrent payment order was initially made on paper, all payments related to this recurrent payment must be reported as non-electronic (element electronic = *false*) even if the subsequent payments are executed electronically.

Card-based payment transactions are considered as electronic (*true*) if they are initiated at an EFTPOS, ATM or other physical terminal that allows electronic payment initiation or remotely by electronic means of information transmission. Card-based payment transactions are considered as non-electronic (*false*) if they are initiated at a physical terminal through a manual authorisation procedure (e.g. imprinters) or via mail order or telephone order (MOTO).

6.5 Channel for giving consent (element channelForGivingConsent)

Direct debits are reported based on the channel used for giving consent (code list 14: channel for giving consent). The reportable categories are as follows:

- Electronic mandate (E)
- Other than electronic mandate (O)

Electronic mandate (E) is a consent given in electronic form.



Other than electronic mandate (O) is a consent given in other than electronic form.

6.6 Card type (element cardType)

Card payments are reported based on card type (code list 4: card type). The reportable types are as follows:

- Debit card (C110)
- Delayed debit card (C120)
- Credit card (C130)
- Card other than a payment card (C900)

Debit card (C110) is a card enabling cardholders to have their purchases directly and immediately charged to their accounts, whether held with the card issuer or not. A card with a debit function may be linked to an account offering overdraft facilities as an additional feature. The number of cards with a debit function refers to the total number of cards in circulation and not to the number of accounts to which the cards are linked. The distinguishing feature of a card with a debit function, in contrast to a card with a credit function or a delayed debit function, is the contractual agreement to charge purchases directly to funds on the cardholder's current account.

Delayed debit card (C120) is a card enabling the cardholder to have purchases (incl. cash withdrawals) charged to an account with the card issuer, up to an authorised limit. The balance in this account is then settled in full at the end of a pre-defined period. The distinguishing feature of a card with a delayed debit function, in contrast to a card with a credit function or a debit function, is the contractual agreement granting a credit line but with an obligation to settle the debt incurred at the end of a pre-defined period. If the card has a credit function, it is not reported here but in category C130, credit card. A delayed debit card is reported as a credit card if the delayed debit function cannot be specified. The same logic applies to the reporting of transactions made with a delayed debit card.

Credit card (C130) is a card enabling the cardholder to make purchases, and in some cases also to withdraw cash, up to a pre-arranged ceiling. The credit granted may be settled in full by the end of a specified period or may be settled in part, with the balance taken as extended credit on which interest is usually charged. The distinguishing feature of a card with a credit function, in contrast to a card with a debit function or a delayed debit function, is the contractual agreement granting the cardholder a credit line allowing for extended credit.

Card other than a payment card (C900) is a card that does not belong to the other categories. It may be, for example, a cash card enabling the holder to withdraw cash from an ATM and/or to deposit cash to an ATM.



6.7 Remote/non-remote (element remoteNonRemote)

Remote/non-remote is reported for credit transfers, card payments and e-money payments (code list 15: remote/non-remote payment). The reportable categories are as follows:

- Remote payment (R)
- Non-remote payment (NR)
- Chip or magnetic stripe (NRP)
- Contactless payment (NRC)

Remote payment (R) is reported for credit transfers, e-money payments and card payments as well as payment transactions reported in the role of PISP. Credit transfers initiated remotely include credit transfers initiated for example via online bank or a mobile banking application as well as credit transfer-based payments initiated with an e-payment button in an e-merchant's website. Card-based remote payments include payment transactions initiated through the internet or other remote communications device without the payer and payee having to be physically present at the same time (card not present, CNP). Remote payments can be made using a card or a mobile payment solution on which card data has been stored. Remote payments include the following card-based payments: e-commerce related payments made on the web (using a card or a mobile payment solution), payments made within mobile solutions (in-app) and P2P (person-to-person) payments. When reporting card payments initiated via mobile payment solutions the following card payments are categorized as remote payments: e-commerce related payments made using a mobile payment solution, payments made within mobile solutions (in-app) and P2P (person-to-person) payments. Hence, when reporting card payments initiated via mobile payment solutions, other mobile payments than those made at merchant premises are remote payments.

Non-remote payment (NR) is only reported for credit transfers and e-money payments. Non-remote payments are reported separately for card payments based on whether the payment is made using the chip (or magnetic stripe) or contactless payment. Non-remote payment comprises payment transactions initiated using a physical terminal (such as a payment terminal, credit transfer ATM, ATM, unattended payment terminal). For example, credit transfers initiated in a credit transfer ATM are reported as electronic payments (element electronic is "true") and non-remote payments (see section 6.14 Terminal). In addition, credit transfer-based payments initiated at a physical POS are reported as non-remote payments.

Chip or magnetic stripe (NRP) includes contact card payments made by reading the chip or magnetic stripe on a card.

Contactless payment (NRC) includes card payments where the payer and payee (and/or their devices) are physically in the same location and communication with a payment instrument and terminal takes place using a contactless payment technology (e.g. NFC, BLE, QR). Contactless payments can be made using a card or a mobile payment solution on which card data has been stored. Hence, contactless payments include, in addition to contactless



payments with physical cards, card-based payments at a physical POS (at merchant premises) using a mobile payment solution based on abovementioned contactless payment technologies.

6.8 Terminal (element terminal)

Cash withdrawals are reported based on the type of terminal (code list 9: type of terminal). The reportable categories are as follows:

- Physical POS (T011)
- ATM (T020)
- Over-the-counter (OTC) (T030)
- Other (T900)

Physical POS (T011) includes cash withdrawals at physical POS terminals.

ATM (T020) comprises cash withdrawals at automated teller machines.

Over-the-counter (OTC) (T030) comprises cash withdrawals made in domestic banks' offices. (OTC = Over-The-Counter)

Other (T900) comprises for example cash ordered via post or cash ordered through cash-in-transit services..

6.9 Customer authentication (element customerAuthentication)

Payment transactions are reported based on the type of authentication (code list 19: strong customer authentication). The reportable categories are as follows:

- Authenticated via strong customer authentication (SCA)
- Authenticated via non-SCA (NSCA)

Authenticated via strong customer authentication (SCA) refers to strong authentication in accordance with Article 4(30) of the Payment Services Directive, based on two or more elements.

Authenticated via non-SCA (NSCA) comprises transactions exempted from strong customer authentication pursuant to Chapter III of Delegated Regulation (EU) 2018/389 as well as transactions for which the provisions in Article 97(1) of the Payment Services Directive do not apply.

6.10 Reason for non-SCA (element reasonForNonSCA)

Payments where strong customer authentication has not been used are reported according to the reason (code list 20: reason for non-SCA). The reportable categories for the use of non-strong customer authentication are based on Commission Delegated Regulation (EU) 2018/389 and are as follows:

- Low value (R01)
- Contactless low value (R02)
- Payment to self (R03)



- Trusted beneficiary (R04)
- Recurring transaction (R05)
- Unattended terminal (R06)
- Secure corporate payment processes and protocols (R07)
- Transaction risk analysis (R08)
- Merchant initiated transaction (R09)
- Other (R99)

Where more than one reason for the use of non-strong authentication is applicable to a payment transaction, the exemption that was applied primarily is the one to report. Reasons for the use of non-strong customer authentication are mutually exclusive.

Low value (R01) refers to situations where the following conditions are met:

- a) the amount of the remote electronic payment transaction does not exceed EUR 30; and
- b) the cumulative amount of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed EUR 100; or
- c) the number of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed five consecutive individual remote electronic payment transactions.

Contactless low value (R02) refers to contactless electronic payment transactions meeting the following conditions:

- a) the individual amount of the contactless electronic payment transaction does not exceed EUR 50; and
- b) the cumulative amount of previous contactless electronic payment transactions initiated by means of a payment instrument with a contactless functionality from the date of the last application of strong customer authentication does not exceed EUR 150; or
- c) the number of consecutive contactless electronic payment transactions initiated via the payment instrument offering a contactless functionality since the last application of strong customer authentication does not exceed five.

Payment to self (R03) comprises credit transfers where the payer and the payee are the same natural or legal person and both payment accounts are held by the same account servicing payment service provider.

Trusted beneficiary (R04) comprises payments where the payee is included in the list of trusted beneficiaries created by the payer.

Recurring transaction (R05) comprises transactions belonging to a series where recurring payments are made to the same payee with the same



amount specified by the payer. When the series of payments is created for the first time or amended, strong customer authentication is used. Other payments in the series do not require strong customer authentication, and hence they are included in this item.

Unattended terminal (R06) comprises electronic payment transactions at an unattended payment terminal for the purpose of paying a transport fare or a parking fee. Payment transactions subject to Article 12 of Commission Delegated Regulation (EU) 2018/389.

Secure corporate payment processes and protocols (R070) comprises circumstances where strong customer authentication is not applied, in respect of legal persons initiating electronic payment transactions through the use of dedicated payment processes or protocols that are only made available to payers who are not consumers, where the competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security to those provided in the Payment Services Directive.

Transaction risk analysis (R08) comprises payment transactions identified by the payment service provider as posing a low level of risk and therefore excluded from strong customer authentication. The conditions of a low level of risk are defined in more detail in Article 18 of Commission Delegated Regulation (EU) 2018/389.

Merchant initiated transaction (R09) refers to “Merchant initiated transaction” as defined in Annex II, Part C, footnote 4 of the EBA Guidelines (EBA/GL/2020/01) amending the EBA Guidelines on reporting requirements for fraud data under Article 96(6) of the Payment Services Directive.

Other (R99) comprises reasons incompatible with other categories not to apply strong customer authentication.

6.11 Fraud type (element fraudType)

Fraudulent payment transactions are reported according to the type of fraud (code list 21: fraud type). The reportable types are as follows:

- Issuance of a payment order by the fraudster (F01)
- Lost or stolen card (F02)
- Card not received (F03)
- Counterfeit card (F04)
- Card details theft (F05)
- Modification of a payment order by the fraudster (F06)
- Manipulation of the payer (F07)
- Unauthorised payment transaction (F08)
- Other (F99)

Issuance of a payment order by the fraudster (F01) comprises fraud where a fake payment order is issued by the fraudster after having obtained the payer's/payee's sensitive payment data through fraudulent means.



Lost or stolen card (F02) comprises fraud with the use of a lost or stolen card-based payment instrument (debit, delayed debit or credit card) without the actual, implied, or apparent authority of the cardholder.

Card not received (F03) comprises fraud using a card that the payer claimed was not received, although the payer's PSP (issuer) confirms it was sent to the payer (by any delivery method).

Counterfeit card (F04) comprises fraud involving the use of an altered or illegally reproduced card-based payment instrument, including the replication or alteration of the magnetic stripe or embossing.

Card details theft (F05) comprises fraud involving theft of sensitive payment data as defined in Article 4(32) of the Payment Services Directive referring to a card-based payment instrument.

Modification of a payment order by the fraudster (F06) refers to fraud where the fraudster intercepts and modifies a legitimate payment order at some point during the electronic communication between the payer's device and the payment service provider or modifies the payment instruction in the payment service provider's system before the payment order is cleared and settled.

Manipulation of the payer (F07) comprises fraud where the fraudster has manipulated the payer to issue a payment order or to give the instruction to do so to the payment service provider, in good faith, to a payment account it believes belongs to a legitimate payee.

Unauthorised payment transaction (F08) includes fraud resulting from the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer.

Other (F99) includes fraud types other than those specified in this field.

6.12 Liability bearer (element liabilityBearer)

Losses due to fraud are reported according to who bears the losses (code list 22: liability bearer). The reportable categories are as follows:

- Reporting PSP (PSP)
- PSU of the reporting PSP (PSU)
- Other (OTH)

Reporting PSP (PSP) comprises transactions where the loss due to fraud is borne by the reporting payment service provider.

Payment service user (PSU) comprises transactions where the loss due to fraud is borne by the reporting payment service user.



Financial Stability and Statistics Department

Financial Statistics Office

25.11.2024

Public

Other (OTH) comprises transactions where the loss due to fraud is borne by another party than the reporter or the reporter's customer.

6.13 Counterparty's PSP location (element counterpartyPSPLocation)

The country of location of the counterparty's payment service provider is reported in this field. The country is reported using the code values in code list *Country (ISO 3666)*.

6.14 Terminal location (element terminalLocation)

The country of location of the terminal used to make the payment transaction is reported in this field. The country is reported using the code values in code list *Country (ISO 3166)*.