



NARODOWY
BANK POLSKI

No. 6.0

Instructions for reporting agents

Payment Statistics Database - BSP System
– BSP

Version 6.0

| | |
|---|----|
| Glossary | 6 |
| 1. Legal basis and rules for preparing reports | 8 |
| 1.1. Legal basis | 8 |
| 1.2. Instructions on how to compile reports – general information | 8 |
| 1.3. Regulation on the detailed scope and procedure of providing information to Narodowy Bank Polski by acquirers, payment instruments issuers and electronic money issuers | 9 |
| 1.3.1. Entities subject to the reporting obligation | 9 |
| 1.3.2. Dates and frequency of reporting data to NBP | 9 |
| 1.3.3. Information concerning filling in the ST forms | 9 |
| 1.3.3.1. Form ST.01 | 9 |
| 1.3.3.2. Form ST.02 | 11 |
| 1.3.3.3. Form ST.03 | 12 |
| 1.3.3.4. Form ST.04 | 12 |
| 1.3.3.5. Form ST.05 | 13 |
| 1.3.3.6. Form ST.06 | 14 |
| 1.3.3.7. Form ST.07 | 15 |
| 1.3.4. Information concerning filling in the FN forms | 16 |
| 1.3.4.1. Form FN.01 | 18 |
| 1.3.4.2. Form FN.03 | 22 |
| 1.3.4.3. Form FN.04 | 23 |
| 1.3.4.4. Form FN.05 | 23 |
| 1.3.4.5. Form FN.06 | 25 |
| 1.3.4.6. Form FN.07 | 25 |
| 1.3.4.7. Form FN.08 | 26 |
| 1.3.4.8. Form FN.09 | 27 |
| 1.3.4.9. Form FN.10 | 29 |

| | |
|--|-----|
| 1.3.4.10. Form FN.12 | 30 |
| 1.3.4.11. Form FN.13 | 31 |
| 1.3.4.12. Form FN.13.1 | 32 |
| 1.3.4.13. Form FN.15 | 32 |
| 1.3.4.14. Form FN.16 | 34 |
| 1.3.4.15. Form FN.17 | 35 |
| 1.3.4.16. Form FN.18 | 35 |
| 1.3.4.17. Form FN.19 | 37 |
| 1.3.4.18. Form FN.20 | 38 |
| 1.4. Regulation of the Minister of Finance of 23 April 2004 on the manner, scope and dates of the provision by entities participating in money settlements and interbank settlements of the data necessary for Narodowy Bank Polski to assess the functioning of money clearing and interbank settlements (Journal of Laws, No. 107, item 1139). | 38 |
| 1.4.1. Clearing houses/payment system operators | 38 |
| 1.4.2. Economic operators pursuing business activity in the field of execution and intermediation in execution of money remittances in domestic and foreign trade | 39 |
| 1.4.3. Poczta Polska S.A. | 39 |
| 2. Information on filling in Forms AR2, WIP2 and AIS/PIS | 41 |
| 2.1. General information | 41 |
| 2.2. Table 4a | 48 |
| 2.2.1. Credit transfer | 50 |
| 2.2.2. Direct debit | 58 |
| 2.2.3. Card-based payment transactions | 59 |
| 2.2.4. Cheques | 64 |
| 2.2.5. E-money payment transactions WPE2/WIPE2 | 65 |
| 2.3. Tables 5 | 70 |
| 2.3.1. Credit transfer | 71 |
| 2.3.2. Direct debit | 75 |
| 2.3.3. Card-based payment transactions | 76 |
| 2.3.4. Cash withdrawal | 81 |
| 2.4. General information on filling in WPE2/WIPE2 forms | 82 |
| 2.5. AIS/PIS | 91 |
| 2.5.1. Detailed information on the reported tables | 93 |
| 3. Access to Payment Statistics Database – BSP system | 98 |
| 3.1. Access to Payment Statistics Database – BSP | 98 |
| 3.2. Access to the test environment of the BSP system | 102 |

| | |
|---|-----|
| 3.3. Useful links | 102 |
| 4. Access to SIS Portal and to AZU | 103 |
| 4.1. First access to SIS Portal and AZU for the BSP system | 103 |
| 4.2. SIS Portal – Working Environment | 104 |
| 4.2.1. SIS Portal User Manual | 105 |
| 4.2.2. Submission of reports via SIS Portal to the BSP system (working environment) | 105 |
| 4.3. AZU – working environment | 107 |
| 5. Requirements for preparation of XBRL files | 110 |
| 5.1. Data submission format | 110 |

Glossary

Acquirer – a provider performing activities of enabling payment transactions, initiated by the merchant or through it, using a payer's payment instrument, in particular involving handling authorisations, transfer, to the payment card issuer or payment schemes of payment orders of the payer or the merchant in order to transfer funds owed to the merchant, with the exception of activities involving transaction clearing and settlement under the payment system in the meaning of the Act on Settlement Finality (acquiring) (Act on Payment Services), Article 2(1a), Article 3(1)(5)).

Merchant – an entity authorised to receive funds in exchange for the delivery of goods or services (Regulation ECB/2013/43). In practice, this is a shop or a merchant location selling goods or services, including a shop selling goods or services via the Internet;

POS terminal – a device allowing the use of payment cards at a physical (not virtual) point of sale (Regulation ECB/2013/43). It is an electronic terminal for authorising payment cards or mobile payments;

Payment instrument – a personalised device or set of procedures agreed between the user and the provider, used by the user for placing payment orders (APS, Article 2(10)); In particular: a credit card, credit transfer (including pay-by-link), direct debit, an instrument enabling making mobile payments, as well as enabling transfers of funds between users with the use of such an instrument;

Cash back – a cash withdrawal made at a cash register at a point of sale during a cashless purchase transaction made with the use of a payment card;

Pay-by-link – a payment method in online banking used by online shops and auction websites. In this method, during a purchase in an online shop, the customer receives a specially generated link by means of which, after logging in to online banking of the customer's bank, the customer receives a prepared, unmodifiable form and finalises the transaction by accepting it;

Card not present – a card transaction which does not require the physical use of a payment card: mail order, telephone order, internet order. These transactions are made on the basis of data provided by the customer (e.g. card number, full name, expiry date, CVV2/CVC2, etc.);

Payment instrument issuer – an entity providing a payment service consisting in issuing payment instruments (APS, Article 2(35a), Article 3(1)(4));

Payment card issuer – a provider issuing a payment card to be used by a payer (APS, Article 2(35c));

Payment card – a card entitling to withdraw cash or submit a payment order through a merchant or an acquirer, accepted by the merchant in order for it to receive funds due to it (APS, Article 2(15a));

Mobile payment – a payment, or a transfer of funds, in which a mobile phone (or a mobile device with similar functions) is used to initiate, confirm and finalise the transaction. Mobile payments do not include processes such as e.g.: placing an order via a mobile phone or delivery of goods or services to the payer's device. Mobile payments also include NFC contactless payments initiated using a phone;

Clearing house – in the meaning of Article 67 of the Banking Act of 29 August 1997 (Journal of Laws of 1997, No. 140, item 939, as amended);

Electronic money (e-money) – electronically, including magnetically, stored monetary value, which is issued, with the obligation of its redemption, on receipt of funds for the purpose of making payment transactions, accepted by entities other than only the electronic money issuer (APS, Article 2(21a)); the activity in the scope of electronic money issuing and its redemption may be performed only by electronic money issuers (APS, Article 4(2a)); electronic money issuers may include the following entities (APS, Article 4(2)(1-4) and (6-8)):

- a domestic bank within the meaning of Article 4(1)(1) of the Banking Act;
- a branch of a foreign bank within the meaning of Article 4(1)(20) of the Banking Act;
- a credit institution within the meaning of Article 4(1)(17) of the Banking Act and, respectively, a branch of a credit institution within the meaning of Article 4(1)(18) of the Banking Act;
- an electronic money institution;
- a payment institution;
- the European Central Bank, Narodowy Bank Polski and the central bank of another Member State – other than acting in their capacity as monetary authorities or public administration bodies;
- a public administration body (APS, Article 4(2b));
- a branch of a foreign electronic money institution;
- a branch of an entity providing postal payment services in the Member State other than the Republic of Poland, authorised in compliance with the law of such a state to issue electronic money and Poczta Polska Spółka Akcyjna to the extent the provision of Article 13(1)(2a) of the Act of 5 September 2008 on commercialisation of a state enterprise of public utility “Poczta Polska” (Journal of Laws No. 180 item 1109, of 2012 item 1529 and of 2013 item 1036) authorises it to issue electronic money;
- a credit union;

APS – the Act on Payment Services of 19 August 2011;

1. Legal basis and rules for preparing reports

1.1. Legal basis

Legal acts regulating the scope of statistical data provided to the Payment System Department of the National Bank Polski:

1. Regulation of the Minister of Finance of 22 December 2022 on providing information to Narodowy Bank Polski by acquirers, payment instruments issuers and electronic money issuers (Journal of Laws, item 2819),
2. Regulation of the Minister of Finance of 19 December 2022 on providing data to Narodowy Bank Polski for the assessment of the functioning of monetary and interbank settlements (Journal of Laws, item 2766).

The information collected from entities provides the basis for aggregating the data according to the requirements defined by the European Central Bank for the euro area and non-euro area member states in the scope of payment statistics. These requirements have been specified in the Recommendation of the European Central Bank of 28 November 2013 on payment statistics (ECB/2013/44) and in the Regulation (EU) 2020/2011 of the European Central Bank of 1 December 2020 amending Regulation (EU) No 1409/2003 on payment statistics (EBC/2013/43)(ECB/2020/59).

Moreover, the data collected by Narodowy Bank Polski enable the Polish central bank to assess periodically the functioning of the Polish payment system.

Selected aggregated statistical data are published on the website of Narodowy Bank Polski <http://www.nbp.pl>.

1.2. Instructions on how to compile reports – general information

The form items that are not applicable to the reporting agent remain blank, i.e. they are not to be filled in with zeros, except for in the following events:

- if in the previous reporting quarter, an item showed a value greater than zero, in the subsequent reporting quarter this item should be filled in with the “0” number,
- the reported “0” value is significant.

The transaction value is shown in full zlotys, up to two decimal places. The value of transactions in foreign currencies should be converted into PLN at the exchange rate of the day on which the transaction was performed. If it is not possible to use the exchange rate of the day on which the transaction was performed, quarterly weighted average exchange rates of foreign currencies published on the NBP website should be adopted for the quarter in which the transactions were performed. Quarterly weighted average exchange rates of foreign currencies can be found at:

[Historic average exchange rates – table A \(CSV, XLS\) | Narodowy Bank Polski - Internetowy Serwis Informacyjny \(nbp.pl\)](#), in tables entitled “Weighted average exchange rates of foreign currencies in PLN”, for CSV format in the line *quarterly, semi-annual, annual* in the column for the relevant quarter, semi-annual period or for CSV format in the sheet “Quarterly” in the column for the relevant quarter, semi-annual period.

1.3. Regulation on the detailed scope and procedure of providing information to Narodowy Bank Polski by acquirers, payment instruments issuers and electronic money issuers

1.3.1. Entities subject to the reporting obligation

The Regulation identifies entities subject to the reporting obligation and defines the scope of the reportable data. The reporting agents provide statistical data in individual forms. The set of individual forms comprises a report. The type of report shall be determined by the reporting agent.

The following entities are subject to the obligation of providing data to NBP:

- acquirers (AR); reports AR1, AR2,
- payment instrument issuers (WIP); reports WIP1, WIP2,
- electronic money issuers (WPE); report WPE2,
- issuers of payment instruments on which electronic money issued by another entity is stored (WIPE); report WIPE2,

Reports are submitted electronically via the web portal of the Financial Information Reporting System (SIS Portal), using the XBRL taxonomy made available by NBP in the web portal of the Financial Information Reporting System.

1.3.2. Dates and frequency of reporting data to NBP

The reports are drawn up on a quarterly basis and submitted to NBP by the end of the last business day of the month following the end of the quarter the data relate to.

1.3.3. Information concerning filling in the ST forms

1.3.3.1. Form ST.01

Number of merchants, including number of points of sale (merchant locations) and number of devices accepting payment cards

The form should specify the number of merchants, the number of points of sale and the number of devices located in the territory of the Republic of Poland and outside the territory of the Republic of Poland.

In items “Number of merchants – Internet” and the “Number of points of sale – Internet”, the localisation “on the territory of the Republic of Poland” or “outside the territory of the Republic of Poland” is determined by the address of the seat of the entity (merchant) which entered into an agreement with the acquirer.

In items “Number of merchants – Internet, of which: merchants equipped with both devices accepting payment cards and solutions supporting payments on the Internet” please indicate the number of merchants that have concluded agreements with the acquirer for the acceptance of payment cards at physical points of sale and via the Internet.

A point of sale on the Internet is equivalent to a website operated by a merchant, which means that a single merchant selling goods and services on the Internet may have several points of sale.

The category “Number of devices” does not apply to entities selling goods or services only via the Internet.

In the category “Number of devices – Devices accepting payment cards” please specify all the devices accepting payment cards. Individual items “[of which:] devices...” (listed eight types of devices) do not add up in the “Number of devices” category because a given terminal may be reported in a number of categories at the same time.

“Devices accepting payment cards, of which: mPOS” shall mean any physical device for payment card transactions which does not have its own communications module and which needs a wireless or cable connection to an external device (e.g. a tablet or phone) in order to make payments, and which does not print transaction confirmations independently. However, it is not a programmable PIN-pad that must be connected to a cash system.

“Devices accepting payment cards, of which: softPOS” shall mean any application installed on a mobile device (e.g. on a smartphone or a tablet), which enables making payments with payment cards. The category “softPOS” is of a non-exclusive nature and includes also such solutions as “PIN on Glass”, “Tap on Phone” and “Cloud POS”.

“Devices accepting payment cards, of which: self-service type” shall mean devices which are unattended, in which a card holder independently initiates and makes a payment (e.g. a vending machine).

In the category “Other”, please provide information on the number of physical devices accepting payment cards other than those specified in categories above.

When reporting the number of devices accepting payment cards located outside the territory of the Republic of Poland, i.e. if the field “Number of devices – Devices accepting payment cards – outside

the territory of the Republic of Poland” has been completed, the number of devices accepting payment cards with a breakdown by individual European Union member states and other countries of the world should be provided in Form ST.04, in the column “Number of devices accepting payment cards”.

Forms ST.01, ST.02 and ST.03 relate to the acceptance network for payment cards, electronic money and payment instruments, respectively. Where a merchant, a point of sale or a device enables accepting payment cards, electronic money and payment instruments at the same time, this information should be reported in all three forms.

The number of merchants, the number of points of sale and the number of devices should be given in units as of the end of the quarter.

1.3.3.2. Form ST.02

Number of merchants, including points of sale, and number of devices accepting electronic money

The form should specify the number of merchants accepting electronic money, the number of points of sale accepting electronic money and the number of devices accepting electronic money located in the territory of the Republic of Poland and outside the territory of the Republic of Poland.

In items “Number of points of sale (merchant locations) accepting electronic money – Internet”, the localisation “on the territory of the Republic of Poland” or “outside the territory of the Republic of Poland” is determined by the address of the seat of the entity (merchant) which entered into an agreement with the acquirer.

A point of sale on the Internet is equivalent to a website operated by a merchant, which means that a single merchant selling goods and services on the Internet may have several points of sale.

The category “Number of devices” does not apply to entities selling goods or services only via the Internet.

In the case of reporting the number of devices accepting cards which store electronic money and the number of devices for charging or discharging of cards with an electronic money function located outside the territory of the Republic of Poland, statistical data with a breakdown by European Union member states and other countries of the world should be provided in form ST.04 in column “Number of devices accepting instruments on which electronic money is stored” and in column “devices for loading and unloading cards with an electronic money function.”

Forms ST.01, ST.02 and ST.03 relate to the acceptance network for payment cards, electronic money and payment instruments, respectively. Where a merchant, a point of sale or a device enables accepting payment cards, electronic money and payment instruments at the same time, this information should be reported in all three forms.

The number of merchants, the number of points of sale and the number of devices should be given in units as of the end of the quarter.

1.3.3.3. Form ST.03

Number of merchants, including number of points of sale, and number of devices accepting payment instruments

The form should specify the number of merchants, the number of points of sale and the number of devices located inside the territory of the Republic of Poland and outside the territory of the Republic of Poland.

Unlike Form ST.01, which relates to the number of merchants, the number of points of sale and the number of devices accepting payment cards, Form ST.03 should state the number of merchants, the number of points of sale and the number of devices accepting payment instruments. The payment instruments category is broader than the payment cards category and in addition to payment cards it includes instruments such as: credit transfers, direct debits, cheques, mobile payments etc.

In items “Number of merchants – Internet” and the “Number of points of sale – Internet”, the localisation “on the territory of the Republic of Poland” or “outside the territory of the Republic of Poland” is determined by the address of the seat of the entity (merchant) that entered into an agreement with the acquirer.

The category “Number of devices” does not apply to entities selling goods or services only via the Internet.

Forms ST.01, ST.02 and ST.03 relate to the acceptance network for payment cards, electronic money and payment instruments, respectively. Where a merchant, a point of sale or a device enables accepting payment cards, e-money and payment instruments at the same time, this information should be reported in all three forms.

A point of sale on the Internet is equivalent to a website operated by a merchant, which means that a single merchant selling goods and services on the Internet may have several points of sale.

The number of merchants, the number of points of sale and the number of devices should be given in units as of the end of the quarter.

1.3.3.4. Form ST.04

Number of devices accepting payment cards and electronic money located outside the territory of the Republic of Poland

The form should contain information on the number of devices accepting payment cards and electronic money located outside the territory of the Republic of Poland, with a breakdown by European Union member states and other countries of the world.

In the form, the item "Number of devices accepting payment cards" corresponds to the item "Number of devices – Devices accepting payment cards – outside the territory of the Republic of Poland" reported in Form ST.01.

In Form ST.04, the item "Number of devices accepting instruments on which e-money is stored" corresponds to item "Number of devices accepting electronic money, of which: - devices accepting instruments on which electronic money is stored – outside the territory of the Republic of Poland" reported in Form ST.02.

In Form ST.04, the item "devices enabling loading and unloading cards with an electronic money function" is equal to the item "Number of devices accepting e-money, of which: - devices for loading and unloading cards with an electronic money function – outside the territory of the Republic of Poland" reported in Form ST.02.

The number of devices should be given in units as of the end of the quarter.

1.3.3.5. Form ST.05

Number and value of cashless payment transactions and cash back transactions made using payment instruments issued on or outside the territory of the Republic of Poland

The form should specify the number and value of cashless payment transactions made using instruments issued on the territory of the Republic of Poland and using instruments issued outside the territory of the Republic of Poland at points of sale operating on the territory of the Republic of Poland.

In the form, the item "Payment cards – issued to individual customers – devices accepting payment cards" and "Payment cards – issued to business customers – devices accepting payment cards" should state the number and value of cashless payment transactions without the cashback service accompanying these transactions. The number and value of cash back services are reported in a separate item in the form.

The item "Payment cards – issued to individual customers – cash back" and "Payment cards – issued to business customers – cash back" should state the number and value of cash back services without the cashless transactions accompanying these services. The number and value of cashless transactions are reported in a separate item in the form.

The item "Internet" should state the number and value of card-not-present transactions.

The item "Credit transfer – Internet" should state the number and value of all credit transfer services.

The item "Credit transfer – of which: via pay-by-link" should state the number and value of credit transfer services performed via pay-by-link. The item "of which: via pay-by-link" is included in item "Internet".

The item "Payment instruments enabling mobile payments" should state the number and value of transactions made in mobile systems such as, e.g.: BLIK, IKO, PeoPay, T-Mobile MyWallet, Orange Cash.

The item "Other payment instruments" should state the number and value of cashless payment transactions made in devices accepting payment instruments and through the Internet which were not reported in other separate categories of this form. For example, this item includes the number and value of transactions made using instruments which enable storing electronic money (e.g. PayPal).

In the case of reporting the number and value of transactions made with payment cards using instruments issued outside the territory of the Republic of Poland, i.e. filling in item "Payment cards – using instruments issued outside the territory of the Republic of Poland", Form ST.06 should be filled in, with transactions broken down by European Union member states and other countries of the world.

The number of cashless payment transactions should be given in units, and the value of cashless payment transactions should be provided in PLN.

"Refunds" shall mean transactions in which a certain amount of funds is transferred to a card of the holder thereof if the holder returns goods (or parts thereof), after the settlement of the initial purchase transaction paid for by card, usually within few days following the transaction day. Chargeback transactions should not be reported. Reversal transactions prior to transaction settlement should not be reported.

1.3.3.6. Form ST.06

Number and value of transactions made at merchants located in the territory of the Republic of Poland using payment cards issued outside the territory of the Republic of Poland

The form should state the number and value of transactions made at merchants located on the territory of the Republic of Poland using payment cards issued outside the territory of the Republic of Poland with a breakdown by individual European Union member states and other countries of the world.

In the form, the sum of items in the columns: "Number of transactions – devices accepting payment cards", "Number of transactions –Internet" and "Number of transactions – cash back" correspond to the respective items "Number of transactions – using instruments issued outside the territory of the Republic of Poland – devices accepting payment cards", "Number of transactions – using instruments issued outside the territory of the Republic of Poland – cash back" and "Number of

transactions – using instruments issued outside the territory of the Republic of Poland – Internet” reported in Form ST.05.

The sum of items in the columns: “Value of transactions – devices accepting payment cards”, “Value of transactions – Internet” and “Value of transactions – cash back” equals the respective items “Value of transactions – using instruments issued outside the territory of the Republic of Poland – devices accepting payment cards”, “Value of transactions – using instruments issued outside the territory of the Republic of Poland – cash back” and “Value of transactions – using instruments issued outside the territory of the Republic of Poland – Internet” reported in Form ST.05.

In the item “Internet” please specify the number and value of card-not-present transactions.

In the form, the item “Payment cards – devices accepting payment cards” should state the number and value of payment transactions made at merchants using payment cards issued outside the territory of the Republic of Poland without the cash back service accompanying these transactions. The number and value of cash back services are reported in a separate item in the form.

The item “Payment cards – cash back” should state the number and value of cash back services without the payment transactions made at merchants using payment cards issued outside the territory of the Republic of Poland accompanying these services. The number and value of the above payment transactions are reported in a separate item in the form.

Item “Rest of the world” should state the aggregate number and value of transactions made in the territory of the Republic of Poland with cards issued outside the territory of the Republic of Poland. The item “Rest of the world” should also be filled in with a breakdown by individual countries, with the use of the list provided by NBP (in the taxonomy these are type-in items).

The value in the item “Rest of the world” should be equal to the value in the item “of which: (country name)”.

The number of transactions should be given in units, whereas the value of transactions should be given in PLN.

1.3.3.7. Form ST.07

Number and value of payment transactions that violated the law or the rules of fair trading and the value of losses incurred by the acquirer and merchants caused by these transactions

The item “Cashless operations – using payment cards” should state the number and value of operations performed using counterfeit cards, stolen cards, lost cards, cards obtained on the basis of false data and cards which have not reached the recipient, and the value of losses caused by these operations.

The item “Cashless operations – using payment cards – of which: Internet” should state the number and value of operations performed via the Internet using counterfeit cards, stolen cards, lost cards,

cards obtained on the basis of false data and cards which have not reached the recipient and the value of losses incurred.

The item “Cashless operations – using payment cards” is the sum of items: “of which: devices accepting payment cards” and “of which: Internet”. The item “of which: chargeback” provides additional information about fraudulent transactions made via the Internet (card-not-present transaction type) as well as in devices accepting payment cards (non-mobile transactions) . Data from this item are also in the following items: “of which: devices accepting payment cards” and “Internet”.

In the item “using payment cards enabling contactless payments” you should only report cashless transactions made with contactless payment cards, smart watches, key rings, etc.

The item “Cashless operations – Other” should state the number and value of fraudulent transactions using other payment instruments, which were not reported in other separate sub-categories within the “Cashless operations” category (e.g. pay-by-link credit transfer operations) as well as the value of losses incurred by the acquirer and merchants as a result of these transactions.

The item “with payment instruments enabling mobile payments (NFC and remote)”, only transactions made with a phone in SIM Centric and HCE technology and using applications such as IKO, PeoPay, BLIK should be reported.

~~If, due to the ongoing complaint procedure, it is not possible to classify a payment transaction as violating the law or fair trading rules in the quarter in which it occurred, please send us information about such transaction in the quarter in which the report is currently prepared.~~

A transaction is reported in a quarter in which it is made and not in a quarter in which it is detected. If a fraudulent transaction is made in Q1 2022 and reported in Q2 2022, a corrected report, including information on the detected fraudulent transaction, shall be submitted for Q1 2022. The date of transaction is decisive. If it turns out that the reported transaction was not fraudulent, a corrected report shall be submitted and the transaction concerned shall be excluded from the statistics for a given quarter.

The number of operations should be given in units and the value of operations should be given in PLN.

1.3.4. Information concerning filling in the FN forms

Additional explanations concerning the data reporting procedure for services such as Google Pay (up to the first quarter of 2022 reported using the Android Pay report), Apple Pay, Garmin Pay, Fitbit Pay and other – Forms FN.01 to FN.08 and FN.15.

1. Form FN.01, which concerns the number of payment cards, should include all cards issued by the issuer according to the criteria indicated, whereas a payment card which is also used to carry out transactions in one of the mobile applications (or in a digital wallet) should be reported as a single card.
 - in the line **“Cards enabling contactless payments”** please report all physical contactless cards,
 - whereas in the line **“Cards installed on the phone, in at least one application (e.g. digital wallet, SIM-NFC)”** please report cards logged in an application,
 - in the line **“Cards installed on other devices enabling contactless payments (gadgets, stickers, etc.)”** cards installed in other devices (gadgets, watches, stickers, etc.) should be reported.

This means that a card used in an application (e.g. a traditional contactless debit card additionally registered in the application) will be reported in Form FN.01 twice: once in the line as a card enabling contactless payments – a traditional card, and again in the second or third line as a card registered in the relevant application.

Moreover, in accordance with the instructions to the forms: In the item **“Cards installed on the phone, in at least one application (e.g. digital wallet, SIM-NFC)”** please specify the number of cards in a mobile payment application (e.g. operating under Google Pay, Apple Pay, etc.) and other solutions based on the NFC technology (e.g. Host Card Emulation).

1. In forms FN.03, FN.05 and FN.07, all transactions executed with the use of payment cards should be reported, including those executed under a payment card-based mobile payment service.
2. In forms FN.04 and FN.06
 - in the line **“Cards enabling contactless payments”** please report transactions made only with the use of physical cards,
 - in the line **“Cards added in at least one application on the phone (e.g. digital wallet, SIM-NFC)”** please report transactions made with the use of cards registered in the mobile application,
 - in the line **“Cards added in other devices enabling contactless payments (gadgets, stickers, etc.)”** cards installed in other devices (gadgets, watches, stickers, etc.) should be reported,
 - in the line **“A payment card without a contactless function installed on the phone enabling contactless payments”** please report payment card transactions made with payment cards without a contactless function which are added to a mobile application installed on a phone equipped with a module enabling contactless payments,

3. In Form FN.15 you should report transactions performed using payment instruments enabling mobile payments (each system separately, providing the name of the system). Thus, in a separate form FN.15 all transactions (number and value) performed with the use of a given application should be reported.

This means that the total number and value of transactions reported in Forms FN.04 and FN.06 in the item **“Cards added in at least one application on the phone (e.g. digital wallet, SIM-NFC)”**, **„Cards added in other devices enabling contactless payments (gadgets, stickers, etc.)”**, **“A payment card without a contactless function installed on the phone enabling contactless payments”** should correspond to the data provided in Form FN.15 concerning the card-based mobile payment systems.

For example, if you offer 3 mobile payment systems, e.g. Google Pay, Apple Pay or Garmin Pay, you are required to fill in Form FN.15 three times, i.e. FN.15 for Google Pay = e.g. 30 units, FN.15 for Apple Pay = e.g. 20 units, FN.15 for Garmin Pay = e.g. 10 units, and in Form FN.04 in the item **“Cards added to at least one application on the phone (e.g. digital wallet, SIM-NFC)”** or **“Cards added in other devices enabling contactless payments (gadgets, stickers, etc.)”** or **“A payment card without a contactless function installed on the phone enabling contactless payments”** for cashless transactions and transactions involving cash, please report the total of the card-based systems.

1.3.4.1. Form FN.01

Number of payment cards issued by the payment instrument issuer

The form should show the number of payment cards with a breakdown by card schemes and by cards issued to individual customers and cards issued to business customers separately for all the card schemes.

A card is a payment instrument based on a unique number that can be used to initiate a payment, cash withdrawal or cash deposit that is processed by a payment card scheme or within the network operated by the issuer of the card. The number can be stored on the physical card, on another device (including a key tag, sticker or smartphone) or can be held virtually without a physical device. Cards offer the cardholder, in accordance with the agreement with the card issuer, one or more of the following functions: cash, debit, delayed debit, credit and e-money. If a physical payment card is added to a digital wallet (digitalised), it shall be recognised as a single card.

In the category **“Cards by function”**:

- the sub-category **“ATM-only cards”** shall indicate the number of cards used exclusively to withdraw cash from ATMs,

- the sub-category “payment cards with the function of cash withdrawal from the ATM” shall indicate the number of cards used to make payments in shops and to withdraw cash from ATMs,
- the sub-category “payment cards without the function of cash withdrawal from the ATM” shall indicate the number of cards used exclusively for making payments in shops.

Debit card, as defined in Article 2(33) of Regulation EU 2015/751, means a category of payment instrument that enables the payer to initiate a debit card transaction, excluding those with prepaid cards. A debit card enables the holder to initiate payment transactions, each of which is recorded on the payer’s account.

Charge card (delayed debit card): A card enabling cardholders to have their purchases charged to an account with the card issuer up to an authorised limit. The balance of this account is then settled in full at the end of a pre-defined period. The holder is usually charged an annual fee.

Credit card, as defined in Article 2(34) of Regulation EU 2015/751, shall mean a category of payment instrument that enables the payer to initiate a credit card transaction.

A distinguishing feature of a charge card (delayed debit card) is that, in contrast to a debit card or a credit card, the charge card is regulated by a credit limit agreement in accordance with which the holder thereof is obliged to pay the total amount of the transactions debited as at the end of a pre-defined period, without interest to be paid. This card is also called a debit card with a delayed payment date.

In the category “Cards by data recording technology” please specify the number of:

- cards equipped only with a magnetic strip,
- cards equipped with an EMV microprocessor and a magnetic strip – cards equipped with both a magnetic strip and a microprocessor in an EMV standard,
- cards equipped only with an EMV microprocessor – payment cards equipped only with an EMV microprocessor. Cards inserted in a sticker, watch, key fob or pendant and similar items and SIM Centric cards in the phone,
- cards equipped only with a microprocessor other than EMV – payment cards issued without the logo of a payment organisation with a microprocessor other than EMV, e.g. cards issued by cooperative banks operating under the name OSKAR,
- virtual cards – cards that do not have a physical equivalent, used for remote payments (shopping on the Internet, MOTO transactions), cards enabling contactless payments by phone in the HCE technology and cards in the biometric technology.

With the exception of the item “payment cards active during the last quarter”, the total number of all payment cards issued by the issuer held by the customer and cards prepared for use (activated,

valid, etc.) should be shown in the form in an appropriate breakdown. Cards not activated by the customer should not be reported.

The item “payment cards active during the last quarter” should show the number of payment cards used for performing at least one cash or cashless transaction during the last quarter.

Cards with combined debit, cash functions and e-money functions shall mean cards issued by a payment service provider with a combination of debit, cash and e-money functions. Furthermore, they are disclosed in the following categories: debit, with a cash function and with an e-money function. They include all the valid cards in circulation which are able to perform all the functions simultaneously.

Card with a contactless payment function: a card enabling the holder to initiate a payment transaction with the use of a special contactless technology, when both the payer and the payee in a payment transaction (or their devices) are present in the same physical place.

In the item “Cards installed on the phone, in at least one application (e.g. digital wallet, SIM-NFC)” please specify the number of cards with a mobile payment application (e.g. Google Pay, Apple Pay) and other solutions based on the NFC technology (e.g. Host Card Emulation).

The item “Cards installed on other devices enabling contactless payments (gadgets, stickers, etc.)” should indicate the number of contactless stickers.

The item “Another card scheme” should show the number of payment cards and the number of cards and other instruments enabling contactless payments which were not reported in the other listed card schemes (i.e. VISA, Mastercard, American Express, Diners Club, issuer's own cards).

The items “Cards by function”, “Cards by transaction settlement method”, “Cards by data recording technology” and “Payment cards issued by the issuer (total)” should state the same number for a given card scheme and the breakdown by consumer and commercial cards.

The number of cards and other instruments enabling contactless payments should be given in units as of the end of the quarter.

Payment card shall mean a card that performs at least one of the following functions: debit function, charge card (delayed debit card) or credit card. This card may also have other functions such as an e-money function, but cards that have an e-money function only do not classify to this category. Cards with only a single function of enabling cash withdrawal/ cash deposit are also excluded from this category.

In the item “Payment cards, of which: debit cards, credit cards, charge cards and prepaid cards” please specify only payment cards that do not have a function of making cash withdrawals/deposits at ATMs or at cash desks in bank outlets (OTC). Cards that have several functions are included in each applicable sub-category. Therefore, the total number of cards with a payment function may be smaller than the sum of cards in card sub-categories. To avoid double-

counting, sub-categories should not be added up.. If a “payment card” offers several functions it is counted in each applicable sub-category.

Within each payment function (i.e. debit, delayed debit and credit function), card-based payment instruments are broken down according to the payment card scheme (PCS) under which they are issued. Co-badged card-based payment instruments are counted for each of the applicable schemes. Therefore, the total number of cards by payment function may be smaller than the sum those cards by PCS. To avoid double-counting, the number of cards by PCS should not be added up.

In the item “Payment cards, of which: debit cards, credit cards, charge cards and prepaid cards”, please specify all the cards that are in circulation regardless of when they were issued and how frequently they are used. A card is included in a given category from the moment it is sent to its holder by the card issuer, regardless of whether the holder has activated it. Cards sent to card holders as renewals of the cards whose validity period was to expire are not included in their relevant category, i.e. they are included therein only at their first issuance.

The number of payment cards should be given in units, as of the end of the quarter.

In Form FN.01:

- the sum of individual items of the category “Cards by function” is equal to the item “Cards by function”,
- the sum of individual items in the category “Cards by transaction settlement method” is equal to the item “Cards by transaction settlement method”,
- the sum of the individual items of the category “Cards by data recording technology” is equal to the item “Cards by data recording technology”,
- the sub-category “Payment cards active during the last quarter” is included in the category “Payment cards issued by the issuer (total)”.

For example, the sum of items of the sub-categories “ATM-only cards”, “Payment cards with the function of cash withdrawal from the ATM”, “Payment cards without the function of cash withdrawal from the ATM” is equal to the item “Cards by function”.

Cards with a cash function shall mean a card enabling the holder to withdraw cash at ATMs and/or to deposit cash in ATMs.

Cards with a cash function are cards used for cash withdrawals. The following cards are not included:

- cards enabling their holders only to initiate payment transactions;
- cards used only for withdrawing and depositing cash at ATMs and which have no name of the payer (i.e. machine-readable cards used to deposit money in the cash deposit machines (CDMs)) are reported only under Total number of cards (regardless of the

number of functions they have) in Table No. 2 of the Regulation. These cards cannot be used at ATMs and therefore they are not reported as cards with a cash function.

1.3.4.2. Form FN.03

Number of operations performed inside and outside the territory of the Republic of Poland using payment cards issued in the territory of the Republic of Poland

The category "Cash transactions inside/outside the territory of the Republic of Poland" should show, in the item "OTC cash withdrawals", the number of cash withdrawal transactions from bank cash desks with the use of a card and a POS terminal. The number of cash withdrawal transactions with delivery to the customer's premises should also be reported under this item (such a service is usually associated with a credit card).

The category "Cash transactions inside/outside the territory of Poland" should show, in the item "other", the number of card transactions involving cash which were not reported under other listed items per type of transaction involving cash (i.e. "ATMs – withdrawals", "OTC cash withdrawals", "cash back"). For example, in item "other", the number of cash deposit transactions in Cash deposit machines (CDMs) and ATMs with a deposit function (excluding transactions in drop boxes) should be reported.

In the item "cash back" please specify the number of cash back transactions without any cashless payment transactions accompanying this service. Cash back transactions should not be reported as cashless transactions using card.

The item "Another card scheme" should show the number of card operations which were not reported in the other listed card schemes (i.e. VISA, Mastercard, American Express, Diners Club, issuer's own cards).

In case of reporting the number of cash and cashless transactions performed outside the territory of the Republic of Poland, i.e. filling in the items "Cash transactions outside the territory of the Republic of Poland" and "Cashless transactions outside the territory of the Republic of Poland", relevant items should be filled in also in Form FN.07, with a breakdown by countries of the European Union and other countries of the world.

In Form FN.03, the sum of items "Cash transactions inside the territory of the Republic of Poland", "Cashless transactions inside the territory of the Republic of Poland", "Cash transactions outside the territory of the Republic of Poland", "Cashless transactions outside the territory of the Republic of Poland" is equal to the item "Number of operations performed with the use of particular card types (total)".

The number of operations/transactions should be given in units.

“Number of refunds performed using card” – “refunds” mean transactions in which a certain amount of funds is transferred to a card of the holder thereof if the holder returns goods (or parts thereof), after the settlement of the initial purchase transaction paid for by card, usually within a few days from the transaction day. Chargeback transactions should not be reported. Reversal transactions prior to transaction settlement should not be reported.

1.3.4.3. Form FN.04

Number of contactless operations performed inside the territory of the Republic of Poland using payment cards and other instruments enabling contactless payments

In the item “Cards added in at least one application ~~installed~~ on the phone” please specify the number of transactions using cards in a mobile payment application and other solutions based on the NFC technology (e.g.: Host Card Emulation).

In the item “cards added in other devices ~~Other media~~ enabling contactless payments (gadgets, stickers, etc.)” should indicate the number of transactions using “contactless” stickers.

The item “Another card scheme” should show the number of transactions/operations which were not reported in the other listed card schemes (i.e. VISA, Mastercard, American Express, Diners Club, issuer's own cards).

In the item “Cash transactions inside the territory of the Republic of Poland – Payment cards without a contactless function installed on the phone enabling contactless payments” please include transactions made with the use of a phone with the contactless payment application installed on it, i.e. a contactless payment instrument other than a contactless payment card (a phone on which a payment card without a contactless function was installed).

In the item “Cashless transactions inside the territory of the Republic of Poland – Payment cards without a contactless function installed on the phone enabling contactless payments” please include transactions made with the use of a phone with the contactless payment application installed on it, i.e. a contactless payment instrument other than a contactless payment card (a phone on which a payment card without a contactless function was installed).

In the form, the sum of the items “Cash transactions inside the territory of the Republic of Poland” and “Cashless transactions inside the territory of the Republic of Poland” is equal to the item “Number of operations performed with instruments enabling contactless payments”.

The number of operations/transactions should be given in units.

1.3.4.4. Form FN.05

Value of operations performed inside and outside the territory of the Republic of Poland using payment cards issued in Poland,

The category "Cash transactions inside/outside the territory of the Republic of Poland" should show in the item "OTC cash withdrawals" the value of cash withdrawals from bank cash desks using a card and a POS terminal. The value of cash withdrawals with delivery to the customer's premises should also be reported under this item (such a service is usually associated with a credit card).

The category "Cash transactions inside/outside the territory of the Republic of Poland" should show in the item "other" the value of card transactions involving cash which were not reported under other listed items broken down by type of cash transaction (i.e. "ATMs – withdrawals", "OTC cash withdrawals", "cash back"). For example, in the item "other", the value of cash deposit transactions in CDMs and ATMs with a deposit function (excluding transactions in drop boxes) should be reported.

The value of cash back transactions should be reported in the item "cash back" without any cashless payment transactions accompanying this service. Cash back transactions should not be reported as cashless transactions using cards.

Item "Another card scheme" should show the value of card operations which were not reported in the other listed card schemes (i.e. VISA, Mastercard, American Express, Diners Club, issuer's own cards).

In case of reporting the value of cash and cashless transactions performed outside the territory of the Republic of Poland, i.e. filling in the items "Cash transactions outside the territory of the Republic of Poland" and "Cashless transactions outside the territory of the Republic of Poland", the relevant items in Form FN.07 should be filled in with a breakdown by countries of the European Union and other countries of the world.

In form FN.05, the sum of items "Cash transactions inside the territory of the Republic of Poland", "Cashless transactions inside the territory of the Republic of Poland", "Cash transactions outside the territory of the Republic of Poland", "Cashless transactions outside the territory of the Republic of Poland" is equal to the item "Total value of operations performed with the use of particular card types".

"Value of refunds performed with the card" shall mean transactions in which a certain amount of funds is transferred to a card of the holder thereof if the holder returns goods (or parts thereof), after the settlement of the initial purchase transaction paid for with the card, usually within a few days from the transaction day (return/refund transactions). Chargeback transactions should not be reported. Reversal transactions prior to transaction settlement should not be reported.

The value of operations/transactions should be expressed in PLN. The value of operations in foreign currencies should be converted into PLN at the exchange rate as of the day on which the transaction was performed..

1.3.4.5. Form FN.06

Value of operations performed inside the territory of the Republic of Poland with the use of issued payment cards enabling contactless payments and with the use of other payment instruments enabling contactless payments

In the item “Cards added in at least one application installed on the phone” please specify the value of transactions using cards with a mobile payment application and other solutions based on the NFC technology (e.g.: Host Card Emulation).

In the item “Cards added in other devices ~~Other media~~ enabling contactless payments (gadgets, stickers, etc.)” you should report the value of transactions performed with the use of contactless stickers.

The item “Another card scheme” should show the value of transactions/operations which were not reported in the other listed card schemes (i.e. VISA, Mastercard, American Express, Diners Club, issuer's own cards).

In the item “Cash transactions inside the territory of the Republic of Poland – Payment cards without the contactless function installed on the phone enabling contactless payments” please report transactions made with the use of a phone with a contactless payment application installed on it, i.e. a contactless payment instrument other than a contactless payment card (a phone on which a payment card without a contactless function was installed).

In the item “Cashless transactions inside the territory of the Republic of Poland – Payment cards without the contactless function installed on the phone enabling contactless payments” please report transactions made with the use of a phone with a contactless payment application installed on it, i.e. a contactless payment instrument other than a contactless payment card (a phone on which a payment card without a contactless function was installed).

In form FN.06, the sum of items “Cash transactions inside the territory of the Republic of Poland” and “Cashless transactions inside the territory of the Republic of Poland” is equal to item “Value of operations performed with instruments enabling contactless payments”.

The value of operations/transactions should be expressed in PLN.

1.3.4.6. Form FN.07

Number and value of cashless and cash transactions executed inside the territory of the Republic of Poland with the use of payment cards issued outside the territory of the Republic of Poland

Form FN.07 should be filled in if items “Cash transactions outside the territory of the Republic of Poland” and “Cashless transactions outside the territory of the Republic of Poland” have been filled in Forms FN.03 and FN.05.

In the item “Rest of the world” you should report the aggregate number and value of transactions made in the territory of the Republic of Poland with cards issued outside the territory of the

Republic of Poland. The item "Rest of the world" should also be presented with a breakdown by individual countries, with the use of the list provided by NBP (in the taxonomy these are type-in items).

In form FN.07:

- the sum of items "Cashless transactions with payment cards – devices accepting payment cards – number of transactions" is equal to the sum of items "Cashless transactions outside the territory of the Republic of Poland – devices accepting payment cards" reported in Form FN.03,
- the sum of the items "Cashless transactions with payment cards – card not present (CNP) – number of transactions" is equal to the sum of the items "Cashless transactions outside the territory of the Republic of Poland – card not present (CNP)" reported in Form FN.03,
- the sum of items "Cash transactions with payment cards – cash withdrawal from an ATM – number of transactions" is equal to the sum of items "Cash transactions outside the territory of the Republic of Poland – ATMs – withdrawals" reported in Form FN.03,
- the sum of items "Cashless transactions with payment cards – devices accepting payment cards – value of transactions" is equal to the sum of items "Cashless transactions outside the territory of the Republic of Poland – devices accepting payment cards" reported in Form FN.05,
- the sum of items "Cashless transactions with payment cards – card not present (CNP) – value of transactions" is equal to the sum of items "Cashless transactions outside the territory of the Republic of Poland – card not present (CNP)" reported in Form FN.05 ,
- the sum of items "Cash transactions with payment cards – cash withdrawal from an ATM – value of transactions" is equal to the sum of the items "Cash transactions outside the territory of the Republic of Poland – ATMs – withdrawals" reported in Form FN.05.

Please specify each country in which transactions were made using a card issued by the issuer.

1.3.4.7. Form FN.08

Number and value of payment transactions using issued payment instruments which violated the law or the rules of fair trading and the amount of losses incurred by the issuer caused by such instruments

In the item "Cash operations – ATM" please report cash withdrawal transactions, and in the item "Cash operations – Other" please include cash back transactions, cash advances and other transactions not included in the item "ATM".

The form should be used to report the number of operations, the value of operations and the value of losses incurred by the issuer on the territory of the Republic of Poland. The item "outside the territory of the Republic of Poland" should not be filled in.

In the item "Payment cards by type of fraud", the sum of the items "using lost/stolen cards", "using cards not received", "using counterfeit cards" and "other" should be entered.

The line "Additional information on fraud" should be left blank.

In the items "cashless transactions with the use of cards executed in the EMV standard" and "cashless transactions with the use of cards executed in a standard other than EMV", the number and value of operations should be reported according to the method of their execution, i.e. in the EMV standard or in a standard other than EMV. In this item, the number of cards used for performing the transaction with the breakdown by cards in the EMV standard and cards in a standard other than EMV should not be reported.

The item "using devices enabling contactless payments" should only be used to report contactless transactions performed with payment cards, watches, key fobs, etc.

In the item "using instruments enabling mobile payments", only transactions performed with the use of a phone in the SIM Centric and HCE technology and with the use of applications such as IKO, PeoPay, BLIK, should be reported.

~~If, due to the ongoing complaint procedure, it is not possible to classify a payment transaction as violating the law or fair trading rules in the quarter in which it occurred, please send us information about such transaction in the quarter in which the report is currently prepared.~~

If at the moment of preparing the report the complaint procedure is pending and the party that has incurred the loss cannot be determined, this item should be left empty. After completion of the complaint procedure, information concerning this event should be sent in the quarter in which the report is currently prepared.

The number of operations should be given in units, whereas the value of operations and the value of losses should be provided in PLN. The value of operations and the value of losses should be converted into PLN at the exchange rate as of the day on which the transaction was executed.

A transaction shall be reported in a quarter in which it was made and not in a quarter in which it was detected. If a fraudulent transaction was made in the first quarter of 2022 and reported in the second quarter of 2022, a corrected report, including information on the detected fraudulent transaction should be submitted for the first quarter of 2022. The date of transaction is decisive. If it turns out that the reported transaction was not fraudulent, a corrected report shall be submitted and the transaction concerned shall be excluded from the statistics for a given quarter.

1.3.4.8. Form FN.09

Number and value of credit transfers executed inside the territory of the Republic of Poland

The number and value of credit transfers executed on the territory of the Republic of Poland initiated by clients of payment service providers should be provided. The form should indicate credit transfers initiated by a natural person/a legal person other than a payment service provider

and transmitted to any payee or initiated by a payment service provider if the payee of the credit transfer is another natural person/a legal person other than the payment service provider.

The form should be used to report all transfers executed in a bank operating on the territory of the Republic of Poland.

The associating bank recognises collective credit and debit documents concerning inter-branch, intra-branch and interbank settlements of the affiliated cooperative banks, where on the one side there is a technical account of the affiliated bank and on the other side there is a current account of the cooperative bank kept by the affiliating bank – as inter-branch/intra-branch settlements.

Credit transfers other than initiated electronically or in paper form: this category includes all credit transfers initiated in non-electronically but not in paper-based form, e.g. mail order or telephone order (MOTO) transactions.

In the item “credit transfer in the SEPA standard”, the number and the value of SEPA credit transfer services in the SEPA standard sent via EuroElixir should be provided.

The form should also take into account the number and the value of credit transfer services executed through ATMs.

In the form:

- the sum of the items “initiated in paper-based form”, “initiated electronically” is equal to the item “credit transfer according to the method of placing the order by the customer”
The item “SEPA credit transfer” provides additional information which is included in item “1. credit transfer according to the method of placing the order by the customer”, therefore it should not be summed up with the other items,
- the sum of the items “internally (within a single provider, e.g. inter-branch, intra-branch)”, “externally (between different payment service providers)” is equal to the item “credit transfer executed:”
- the sum of the items “individual customers”, “business customers” is equal to the item “credit transfer executed by:”

In form FN.09, the item “credit transfer according to the method of placing the order by the customer” is equal to the item “credit transfer executed:” and the item “credit transfer executed by:”.

The form should state the number and value of credit transfers executed inside the territory of the Republic of Poland, both in domestic currency and in foreign currencies.

The number of credit transfer services should be given in units, whereas the value of credit transfer services should be provided in PLN. The value of credit transfer services in foreign currencies should be converted into PLN at the exchange rate as of the day on which the service was

performed. If it is not possible to use the exchange rate of the day on which the transaction was performed, quarterly weighted average exchange rates of foreign currencies published on the NBP website should be adopted for the quarter in which the transactions was performed. Weighted average exchange rates of foreign currencies can be found on the website [Historic average exchange rates – table A \(CSV, XLS\) | Narodowy Bank Polski - Internetowy Serwis Informacyjny \(nbp.pl\)](https://nbp.pl), in the “Weighted average exchange rates in PLN” file for the relevant year, in the “Quarterly” files. Transactions in foreign currencies performed on the territory of the Republic of Poland, after conversion into PLN, in accordance with the above guidelines, should be added to transactions executed in PLN.

Cash deposits at the bank cash desks which require the transfer of funds to a bank account maintained by a bank other than the bank accepting the cash deposit are also considered as the credit transfer service. In the form you should state the number and the value of credit transfer services performed in the above mentioned manner.

Cash deposits to the bank account operated by a bank which accepts a cash deposit are recognised as a credit transfer service if the beneficiary is a customer other than the customer making the cash deposit. Cash deposit operations to the customer's own account are not recognised as credit transfers. Cash deposits to bank accounts held by the bank branch made by customers other than the owners of the accounts concerned shall be recognised as a credit transfer service.

A withdrawal / repayment of a loan / payment of a loan instalment / transfer to a term deposit account, i.e. a transaction of transfer of funds between two accounts held by the same customer (e.g. from a personal account (ROR) to a loan or deposit account) as well as accrued interest on the account balance, account maintenance fees, etc., should not be reported.

Please report BLIK type P2P transactions; other BLIK operations should not be reported in the credit transfer category.

1.3.4.9. Form FN.10

Number and value of credit transfer orders sent outside of the territory of the Republic of Poland and received from outside the territory of the Republic of Poland

Use the form to report the number and value of credit transfers ordered to be sent outside the territory of the Republic of Poland (sent abroad) and received from outside the territory of the Republic of Poland (received from abroad). The item shall indicate credit transfer transactions initiated by a natural person/a legal person other than a payment service provider and transmitted to any payee and credit transfers initiated by a payment service provider if the payee of the credit transfer is another natural person/ a legal person other than the payment service provider.

In Form FN.10, the sum of the items “initiated in paper-based form”, “initiated electronically” is equal to the item “credit transfer according to the method of placing the order by the customer”.

The item “SEPA credit transfer” provides additional information contained in the item “1. credit transfer according to the method of placing the order by the customer”, therefore it should not be summed up with the other items.

Cash deposits at the bank cash desks which require the transfer of funds to a bank account maintained by a bank other than the bank accepting the cash deposit are also considered as the credit transfer service. In the form you should state the number and the value of credit transfer services performed in the above mentioned manner.

Cash deposits to the bank account operated by a bank which accepts a cash deposit are recognised as a credit transfer service if the beneficiary is a customer other than the customer making the cash deposit. Cash deposit operations to the customer's own account are not recognised as credit transfers. Cash deposits to bank accounts held by a bank branch made by customers other than the owners of the accounts concerned shall be recognised as credit transfer services.

The number of credit transfer services should be given in units, whereas the value of credit transfer services should be provided in PLN. The value of credit transfer services in foreign currencies should be converted into PLN at the exchange rate as of the day on which the transaction was performed. If it is not possible to use the exchange rate of the day on which a transaction was performed, quarterly weighted average exchange rates of foreign currencies published on the NBP website should be adopted for the quarter in which the transaction was performed. Weighted average exchange rates of foreign currencies can be found on the website [Historic average exchange rates – table A \(CSV, XLS\) | Narodowy Bank Polski - Internetowy Serwis Informacyjny \(nbp.pl\)](https://www.nbp.pl/serwis/informacyjny/interaktywne/tablica/1), in the “Weighted average exchange rates in PLN” file for the relevant year, in the “Quarterly” file.

A withdrawal / repayment of a loan / payment of a loan instalment / transfer to a term deposit account, i.e. a transaction of transfer of funds between two accounts held by the same customer (e.g. from a personal account (ROR) to a loan or deposit account) as well as accrued interest on the account balance, account maintenance fees, etc., should not be reported.

1.3.4.10. Form FN.12

Number and value of direct debits performed inside the territory of the Republic of Poland

In Form FN.12, in the item “direct debit according to the method of placing the order by the customer” should indicate the number and value of direct debit services performed inside the territory of the Republic of Poland in both domestic and foreign currencies (SEPA).

In the form, the number and value of direct debit transactions performed inside the territory of the Republic of Poland is reported by the creditor bank initiating the transaction (instead of the payer/debtor bank). No information should be provided concerning operations between the customer's account and the bank's own account, e.g. loan repayment, increasing savings deposits.

In the form:

- the item “of which: SEPA direct debit” is included in the item “direct debit according to the method of placing the order by the customer”,
- the sum of the items “internally (within a single provider, inter-branch)”, “externally (between different payment service providers)” is equal to the item “direct debit executed:”
- the item “direct debit according to the method of placing the order by the customer” is equal to the item “direct debit executed”.

The number of direct debit services should be given in units, whereas the value of direct debit services should be provided in PLN. The value of direct debit services in foreign currencies should be converted into PLN at the exchange rate as of the day on which the service was performed. If it is not possible to use the exchange rate of the day on which the transaction was performed, quarterly weighted average exchange rates of foreign currencies published on the NBP website should be adopted for the quarter in which the transactions was performed. Weighted average exchange rates of foreign currencies can be found on the website [Historic average exchange rates – table A \(CSV, XLS\) | Narodowy Bank Polski - Internetowy Serwis Informacyjny \(nbp.pl\)](#), in the “Weighted average exchange rates in PLN” file for the relevant year, in the “Quarterly” files.

1.3.4.11. Form FN.13

Number and value of direct debits orders sent outside the territory of the Republic of Poland and received from outside the territory of the Republic of Poland

The item “Orders sent outside the territory of the Republic of Poland” should indicate the number and value of direct debit services as a result of which an account with a Polish bank was credited and an account with a foreign bank was debited. In this item, the Polish bank reports as a beneficiary (recipient) bank.

The item “Orders received from outside the territory of the Republic of Poland” should provide the number and value of direct debit services as a result of which an account with a Polish bank was debited and an account with a foreign bank was credited. In this item, the Polish bank reports as a debtor (payer) bank.

The item “direct debits according to the method of placing the order by the customer ” (refers to columns: “number” and “value”) should contain statistical information on total direct debits .

The number of direct debit services should be given in units, whereas the value of direct debit services should be provided in PLN. The value of direct debit services in foreign currencies should be converted into PLN at the exchange rate as of the day on which the service was performed. If it is not possible to use the exchange rate of the day on which the transaction was performed, quarterly weighted average exchange rates of foreign currencies published on the NBP website should be adopted for the quarter in which the transactions were performed. Weighted average exchange rates of foreign currencies can be found on the website [Historic average exchange rates](#)

[– table A \(CSV, XLS\) | Narodowy Bank Polski - Internetowy Serwis Informacyjny \(nbp.pl\)](#), in the “Weighted average exchange rates in PLN” file for the relevant year, in the “Quarterly” sheet.

1.3.4.12. Form FN.13.1

Number and value of fraudulent credit transfers performed on the territory of the Republic of Poland

In Form 13.1 you should report the number and value of fraudulent credit transfers broken down by the method of their initiation: in paper-based form, electronically or other.

Credit transfers other than those initiated electronically or in paper-based form: this category covers all cases of credit transfers which are initiated non-electronically but not in paper-based form, e.g. mail order or telephone order (MOTO) transactions.

The item „of which: Instant payments” is a sub-category of the item „Initiated electronically”.

1.3.4.13. Form FN.15

Number and value of transactions executed with payment instruments enabling mobile payments

In the form you should not report the number and value of transactions executed through the credit transfer service which is initiated by means of a telephone as an access tool to electronic banking.

The form should state the number and value of transactions using all instruments enabling the execution of mobile payments, separately for each system (e.g.: BLIK, IKO, PeoPay, iKasa, etc.).

In the case of a bank that offers different mobile payment systems, the form must be filled in separately for each system. Each form must be completed with the System name which is provided under the Name of the issuer.

In item “Remote transactions”, please provide the number and value of transactions executed with the use of instruments enabling mobile payments of the type “card not present”.

The number of users is the number of people who have activated BLIK

The number of active users is the number of user who in the reporting period used BLIK at least once and who were the reporting agent’s PSUs on the last business day in the period concerned.

The number of transactions should be given in units, whereas the value of transactions should be given in PLN.

Additional explanations on how to report data for services such as Google Pay (name in the form: Android Pay), Apple Pay, Garmin Pay, Fitbit Pay and others.

Statistical data concerning such services should be reported in forms FN.01 – FN.08 and FN.15.

1. Form FN.01, which concerns the number of payment cards, should include all cards issued by the issuer according to the criteria indicated; a payment card which is also used to carry out transactions in one of the applications should be reported as a single card.
2. In Form FN.01:
 - in the line **“Cards enabling contactless payments”** all physical contactless cards should be reported
 - and in the line **“Cards installed on the phone (e.g. digital wallet, SIM-NFC)”** cards logged in an application should be reported.

or

- in the line **“Cards installed on other devices enabling contactless payments”** (gadgets, stickers, etc.) cards installed in other devices should be reported

This means that a card used in an application (e.g. a traditional contactless debit card additionally registered in the application) will be reported in Form FN.01 twice: once in the first line as a card enabling contactless payments – a traditional card, and again – in the second or third line as a card registered in the relevant application.

Moreover, in accordance with the instructions to the forms: **“The item **“Cards installed in the phone (e.g. SIM-NFC)”** should specify the number of cards with a mobile payment application (e.g.: operating within Orange Cash, T-Mobile MyWallet) and other solutions based on NFC technology (e.g.: Host Card Emulation).”** This also includes Google Pay (name in the form: Android Pay) and other similar services.

3. In forms FN.03, FN.05 and FN.07, all transactions executed using payment cards should be reported, including those executed under a card-based mobile payment service.
 4. In forms FN.04 and FN.06
 - in the line **“Cards enabling contactless payments”** please specify transactions made only using physical cards,
 - whereas in the line **“Cards added to at least one application on the phone (e.g. digital wallet, SIM-NFC)”** transactions performed using cards registered in an application should be reported
- or
- in the line **“Cards added in other devices enabling contactless payments”** (gadgets, stickers, etc.) cards installed in other devices should be reported
5. In Form FN.15 you should report transactions performed with payment instruments enabling mobile payments (each system separately, providing the name of the system). Thus, in a separate form FN.15 all transactions (number and value) performed with each individual application should be reported.

This means that the total number and value of transactions included in forms FN.04 and FN.06 in the item “cards added in at least one application in the phone (e.g. digital wallet, SIM-NFC)” or in the item “cards added in other devices enabling contactless payments” should correspond to the data contained in form(s) FN.15 referring to mobile payment systems based on payment cards.

For example, if you offer 3 mobile payment systems, e.g. Google Pay (Android Pay), Apple Pay or Garmin Pay, you are required to fill in Form FN.15 three times, i.e. FN.15 for Android Pay = e.g. 30 units, FN.15 for Apple Pay = e.g. 20 units, FN.15 for Garmin Pay = e.g. 40 units, whereas in form FN.04 in the item “cards added in at least one application on the phone (e.g. digital wallet, SIM-NFC)” or “cards added in other devices enabling contactless payments” [for cashless transactions and transactions involving cash], the sum of card-based systems should be reported.

1.3.4.14. Form FN.16

Number of ATMs

The form should be filled in by ATM operators (owners of ATMs), both banks and non-bank operators.

In the item “ATMs”, the number of ATMs enabling cash withdrawals and ATMs enabling cash withdrawals and deposits must be provided in aggregate form.

In the form, the sum of the items “enabling cash withdrawals” and “enabling cash withdrawals and deposits” must be equal to the item “ATMs”.

In the item “with a credit transfer function”, you should report the number of ATMs which are equipped with an additional function, i.e. making a credit transfer. The number of ATMs provided in this item is not a separate component of the total number of ATMs; it is only an additional information. ATMs presented in this item are also presented in the items “enabling cash withdrawals” and “enabling cash withdrawals and deposits”.

In Form FN.16:

- the item “enabling cash withdrawals” refers to ATMs with one function – cash withdrawals only,
- the item “enabling cash withdrawals and deposits” refers to ATMs with two functions – cash withdrawals and cash deposits,
- the item “with a credit transfer function” refers to ATMs which, in addition to the cash withdrawal function (refers also to ATMs with two functions), have an additional function enabling the execution of a credit transfer.

The form should state the number of ATMs located inside the territory of the Republic of Poland and located outside the territory of the Republic of Poland.

In the item “enabling cash deposits (cash deposit machines)”, no information about “drop boxes” should be provided.

In the case of reporting the number of ATMs located outside the territory of the Republic of Poland, i.e. filling in the item “Located outside the territory of the Republic of Poland”, please fill in columns “ATMs – number”, “of which: devices enabling cash withdrawals” and “of which: devices with a credit transfer function” and “of which: accepting cashless transactions” in Form FN.17, with a breakdown into particular countries of the European Union and other countries of the world.

The number of ATMs should be given in units according to the status as of the end of the quarter.

1.3.4.15. Form FN.17

Number of ATMs located outside the territory of the Republic of Poland – detailed information

In the item “Rest of the world”, the number of ATMs located outside the territory of the Republic of Poland should be provided in aggregate form, not broken down by individual countries of the world.

In the form:

- the sum of the items “ATMs – number” is equal to the item, “ATMs: - located outside the territory of the Republic of Poland” reported in Form FN.16,
- the sum of the items “of which: devices enabling cash withdrawals” is equal to item “ATMs: - of which: enabling cash withdrawals – located outside the territory of the Republic of Poland” reported in Form FN.16,
- the sum of items “of which: devices with a credit transfer function” is equal to the item “ATMs: - of which: devices with a credit transfer function – located outside the territory of the Republic of Poland” reported in Form FN.16.

The number of ATMs should be given in units according to the status as of the end of the quarter.

1.3.4.16. Form FN.18

Number and value of transactions performed in ATMs located inside and outside the territory of the Republic of Poland

The form should be filled in by ATM operators (owners of ATMs), both banks and non-bank operators.

The form should indicate the number and value of transactions performed in ATMs inside the territory of the Republic of Poland for transactions executed using payment instruments issued by

domestic payment service providers and foreign payment service providers, and outside the territory of the Republic of Poland for transactions performed using payment instruments issued only by domestic payment service providers.

In Form FN.18, the items:

- “Number of transactions – outside the territory of the Republic of Poland – Transactions executed using payment instruments issued by foreign payment service providers, of which – cash withdrawal – cash deposit – credit transfer – purchase of goods or services – other”,
- “Value of transactions – outside the territory of the Republic of Poland – Transactions executed using payment instruments issued by foreign payment service providers, of which – cash withdrawal – cash deposit – credit transfer – purchase of goods or services – other”.

should be left blank.

These items in the form are marked as inactive.

In the form:

- the sum of the items “cash withdrawal”, “cash deposit”, “credit transfer”, “purchase of goods and services” and “other” is equal to the item “Transactions executed using payment instruments issued by domestic payment service providers, of which:”,
- the sum of the items “cash withdrawal”, “cash deposit”, “credit transfer”, “purchase of goods and services” and “other” is equal to the item “Transactions executed using payment instruments issued by foreign payment service providers, of which:”.

In the item "other", the number and value of transactions executed in ATMs which have not been reported in other listed types of transactions executed in ATMs should be provided.

The number and value of cash deposit transactions to drop boxes should not be reported in the item “cash deposit (including drop boxes)”.

In the item “cash deposit (including drop boxes)”, the number and value of cash deposit transactions in devices enabling cash deposits, i.e. cash deposit machines (Cash-in machines) should be reported if a payment card was used to perform the transaction.

In case of reporting the number and value of transactions performed in ATMs inside the territory of the Republic of Poland with the use of payment instruments issued by foreign payment service providers, i.e. filling in the item “Number of transactions – inside the territory of the Republic of Poland – Transactions executed using payment instruments issued by foreign payment service providers, of which:” and “Value of transactions – inside the territory of the Republic of Poland – Transactions executed using payment instruments issued by foreign payment service providers, of which:”, the columns “Number of transactions” and “Value of transactions” should be filled in

Form FN.19, with the breakdown by individual countries of the European Union and other countries of the world.

In the Regulation of the Minister of Finance of 15 October 2014 on the detailed scope and procedure of reporting information to Narodowy Bank Polski by acquirers, issuers of payment instruments and issuers of electronic money and in Annex No. 2 to the aforementioned Regulation, the “*” sign was incorrectly placed after the item “outside the territory of the Republic of Poland”. The “*” sign should have been placed after the item “Transactions executed using payment instruments issued by foreign payment service providers, of which:” i.e. “Transactions executed using payment instruments issued by foreign payment service providers, of which: *”, and the correct reference to Form FN.19 below should read as follows:

“* If you fill in the item “inside the territory of the Republic of Poland – Transactions executed using payment instruments issued by foreign payment service providers”, please fill out also Form FN.19.”

The aforementioned change was introduced in the form – “Transactions executed using payment instruments issued by foreign payment service providers, of which: *”, „*“

If you fill in the item “inside the territory of the Republic of Poland – Transactions executed using payment instruments issued by foreign payment service providers”, please fill out also Form FN.19.”.

The number of transactions performed in ATMs should be given in units, whereas the value of transactions performed in ATMs should be provided in PLN. It should be converted into PLN at the exchange rate as of the day on which the transaction was executed.

1.3.4.17. Form FN.19

Number and value of transactions executed in ATMs located inside the territory of the Republic of Poland using payment instruments issued outside the territory of the Republic of Poland

The form should be filled in by ATM operators (owners of ATMs), both banks and non-bank operators.

In the form:

- the items in the column “Number of transactions” are equal to the item “Transactions executed using payment instruments issued by foreign payment service providers”, respectively, for the items “cash withdrawal”, “cash deposit”, reported in Form FN.18,
- the items in the column “Value of transactions” are equal to the item “Transactions executed using payment instruments issued by foreign payment service providers”, respectively, for the items “cash withdrawal”, “cash deposit”, reported in Form FN.18 .

Within the item “Rest of the world”, the number and value of transactions performed inside the territory of the Republic of Poland using cards issued outside the territory of the Republic of Poland should be provided in an aggregate form. The item “Rest of the world” should also be provided with the breakdown by country, using the list provided by NBP (in the taxonomy these are type-in items).

1.3.4.18. Form FN.20

Number and value of payment transactions registered at ATMs and violating the law or the rules of fair trading, which were executed using issued payment instruments, and the amount of losses incurred by the ATM owner

The form should be filled in by ATM operators (owners of ATMs), both banks and non-bank operators.

In the form, the sum of the items “with payment instruments issued by domestic payment service providers, of which:” and “with payment instruments issued outside the territory of the Republic of Poland” is equal to the item “Cash operations”.

The number of fraudulent operations should be given in units, whereas the value of fraudulent operations and the value of losses incurred by the ATM owner should be provided in PLN.

1.4. Regulation of the Minister of Finance of 19 December 2022 on the provision of the data necessary for Narodowy Bank Polski to assess the functioning of money clearing and interbank settlements (Journal of Laws, item 2766).

The following entities are subject to the obligation to report to NBP:

- clearing houses/payment system operators;
- economic operators pursuing business activity in the field of execution and intermediation in execution of money remittances in domestic and foreign trade;
- state-enterprise of public utility – Poczta Polska.

1.4.1. Clearing houses/payment system operators

Forms for entities whose area of activity comprises clearing and payment services, operating under Article 67 of the Banking Act, are developed based on the type and scope of business activity conducted. A single entity may transfer more than one form where it operates more than one payment system. Narodowy Bank Polski develops templates of forms corresponding to the scope of services offered by a particular entity.

The reports are drawn up on a quarterly basis and submitted to NBP by the end of the last business day of the month following the end of the quarter the data relate to.

If it is not possible to submit data directly through the SIS Web portal, the data may be submitted in writing or via electronic mail.

1.4.2. Economic operators pursuing business activity in the field of execution and intermediation in execution of money remittances in domestic and foreign trade

Information is submitted by economic operators pursuing business activity in the field of execution and intermediation in execution of money remittances in national and foreign trade.

The funds are transferred using the service of domestic or international money remittances (transactions sent abroad and transactions received from abroad). The funds transferred may be delivered for personal collection at the outlet of the particular entity or in an ATM (cash withdrawal), to a payment account (APS, Article 2(25)).

Pursuant to Article 4(22) of Directive EU 2366/2015 'money remittance' 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.

Money remittances are not recognised as credit transfers or reported as other payment services, because they are reported separately. Money remittances are not restricted to money transfers that include cash for both sides of the transaction.

Money remittances sent are reported by the payer's service provider, and money remittances received are disclosed by the payee's service provider.

Any transactions that are related to the payer's or payee's payment account are excluded from the category of money remittances. Such transactions are recognised as part of the relevant payment instrument used.

The number of transactions executed should be given in units, whereas the value of transactions should be provided in PLN.

The reports are drawn up on a semi-annual basis and submitted to NBP by the end of the last business day of the month following the end of the semi-annual period to which the data relate.

If it is not possible to submit data directly through the SIS Web portal, the data can be submitted by e-mail.

1.4.3. Poczta Polska S.A.

The form should provide the number and value of transactions in the scope of services related to performing postal remittances, postal payment orders and cash deposits to bank accounts executed through Poczta Polska S.A.

The number of transactions executed should be given in units, whereas the value of transactions should be provided in PLN.

The reports are drawn up on a semi-annual basis and submitted to NBP by the end of the last business day of the month following the end of the semi-annual period to which the data relate.

The data are submitted electronically via the web portal of the Reporting Information System, using the XBRL taxonomy made available by NBP on the web portal of the Reporting Information System.

2. Information on filling in Forms AR2, WIP2 and AIS/PIS

2.1. General information

On 1 December 2020, the Governing Council of the European System of Central Banks (ESBC) adopted Regulation (EU) of the European Central Bank of 1 December 2020 amending Regulation (EU) No. 1409/2003 on payment statistics (EBC/2013/43)(ECB/2020/59)¹. In the ECB Recommendation of 28 November 2013 on payment statistics (ECB/2013/44), the ECB recommends that central banks of non-euro area member states report on payment statistics to the ECB, in keeping with the new Regulation.

Geographical distribution

| Geo 0 | Geo 1 | Geo 2 | Geo 3 | Geo 4 | Geo 6 |
|----------|------------------------------------|--------------|------------------------------|------------------------------|------------------------|
| Domestic | | | Domestic | Domestic | |
| | Domestic and cross-border combined | Cross-border | By the EEA countries | Cross-border within the EEA | By countries worldwide |
| | | | Cross-border outside the EEA | Cross-border outside the EEA | |

For all payment instruments other than the card-based payment instruments, the residence of the counterparty institution is reported in accordance with the breakdown in Geo 3. For the card-based payment transactions and for cash withdrawals using card-based payment instruments, in addition to the residence of the counterparty institution also the location of the point of sale is reported broken down according to Geo 3. For a specific case of reporting by PISP, the geographical distribution should be reported based on the registered office of the institution holding the account from which the payment is initiated, in order to demonstrate the extent to which the service is provided across borders.

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R2011&from=EN>

For the geographical breakdown according to GEO6, the reporting entity reports only the selected columns of the table, i.e. countries accordingly to the country of an issuer, card or terminal (“typed-in” positions).

Tables with the heading “Person preparing the report” shall include information on persons responsible for the contents of the reports prepared.

The structure of forms filled in by particular entities has been presented below.

| | | |
|--|-----------------|--|
| <p>Number and value of transactions settled by the payment instrument issuers by payment service:</p> <p>1. Credit transfers, direct debits, cheques 2. Card-based payment transactions in devices accepting payment cards by:</p> <p>2.1 the acquirer's country of residence (the name of the table specifies the country). The geographical distribution concerns countries within the EEA, each country separately and collectively for other countries worldwide outside the EEA (so-called GEO3 breakdown); 2.2 the country of location of the terminal (the table columns by GEO3 countries). 2.3 electronic and non-electronic initiation channel and remote and non-remote transactions (the table's site). Electronic non-remote transactions are broken down into payment schemes (e.g. Mastercard, VISA), authenticated by Strong Customer Authentication or via non-Strong Customer Authentication. For transactions without strong customer authentication, please provide information on the reasons why SCA has not been applied.</p> <p>3. cash withdrawal using a card-based payment instrument by:</p> <p>3.1 the acquirer's country of residence (the name of the table specifies the country). The geographical breakdown concerns countries within the EEA, each country separately and collectively for other countries worldwide outside the EEA (so-called GEO3 breakdown); 3.2 the country of location of the terminal (the table columns by GEO3 countries). 3.3 payment schemes (e.g.: Mastercard, VISA) and by card type.</p> <p>Transactions sent reported by owners, holders or operators of ATMs:</p> <p>Number and value of card-based payment transactions at ATMs operated by owners, holders or operators of ATMs, by:</p> <p>4.1 the country of location of the device (the name of the table specifies the country). The information reported concerns transactions</p> | 4a.L | Number and value of transactions – credit transfers, direct debits, cheques. |
| | 4a.W | <ul style="list-style-type: none"> credit transfers are counted on the side of the payer/debtor/sender the sender (“sent”) is an entity that sends funds, e.g. the payer’s/debtor’s bank, and the receiving party (“received”) is the entity receiving funds, e.g. the creditor’s bank; direct debits are counted on the side of the payee the sending party (“sent”) is an entity sending a direct debit and simultaneously receiving/obtaining funds, e.g. the creditor’s bank/ funds recipient’s bank, and the receiving party (“received”) is the entity receiving a direct debit and simultaneously sending the funds, e.g. the payer’s/debtor’s bank; |
| | 4a.S.L_PLiW2 | <p>Transactions sent. The number and value of transactions made with the use of the Issuer’s cards and executed by domestic acquirers (by residents) and cash withdrawals using card-based payment instruments of the Issuer settled by domestic acquirers (by residents)</p> |
| | 4a.S.W_PLiW2 | |
| | 4a.S.L_krajGEO3 | <p>Transactions sent. The number and value of transactions with the Issuer’s cards and executed by foreign acquirers (by non-residents) and cash withdrawals using the Issuer’s cards settled by foreign acquirers (by non-residents).</p> <p>A breakdown by the country of residence of a foreign acquirer executing card transactions is reported separately in individual tables, i.e. using the following forms:</p> <p>4a.S.L_AT (number of transactions settled by the Austrian acquirer), 4a.S.W_AT (value of transactions settled by the Austrian acquirer), 4a.S.L_BE (number of transactions settled by the Belgian acquirer), 4a.S.W_BE (value of transactions settled by the Belgian acquirer), ..., 4a.S.L_G1 (number of transactions settled by the acquirer from outside the EEA), 4a.S.W_G1 (value of transactions settled by the acquirer from outside the EEA).</p> |
| | 4a.S.W_krajGEO3 | |
| | 4a.R.L_PLiW2 | <p>Transactions executed at ATMs located in Poland [received] –</p> <p>Number and value of card-based transactions made at ATMs serviced by their owners, holders or operators.</p> |
| | 4a.R.W_PLiW2 | |
| | 4a.R.L_krajGEO3 | |

| | | |
|---|--|---|
| <p>made in devices in countries within the EEA, each country separately, and collectively for other countries worldwide outside the EEA (by GEO3);</p> <p>4.2 the country of the card issuer (the table columns by GEO3 countries).</p> <p>4.3 electronic and non-electronic initiation channel and initiated via remote and non-remote payment channel (the table's site). In addition the electronic non-remote transactions are grouped under payment schemes, by strong customer authentication and by -non-strong customer authentication. For transactions authenticated via non-Strong Customer Authentication, please provide information on reasons why SCA has not been applied.</p> | 4a.R.W_krajGEO3 | <p>Number and value of card-based transactions made at ATMs serviced by their owners, holders or operators. Transactions received made at ATMs in countries that form part of the EEA and collectively in other countries outside the EEA (by GEO3). Each country of the ATM's location is reported separately in individual tables, i.e. using the following forms:</p> <p>4a.R.L_AT (number of transactions in devices on the territory of Austria),</p> <p>4a.R.W_AT (value of transactions in devices on the territory of Austria),</p> <p>4a.R.L_BE (number of transactions in devices on the territory of Belgium),</p> <p>4a.R.W_BE (value of transactions in devices on the territory of Belgium),</p> <p>....,</p> <p>4a.R.L_G1 (number of transactions in devices in countries outside the EEA),</p> <p>4a.R.W_G1 (value of transactions in devices in countries outside the EEA).</p> |
| <p>Number and value of fraudulent transactions concerning:</p> <ol style="list-style-type: none"> credit transfers, direct debits, cheques card-based payment transactions in devices accepting payment cards cash withdrawals using card-based payment instruments made as card-based transactions at ATMs serviced by their owners, holders or operators <p>The data is provided for exactly in the same way as it is shown in tables 4a, and additionally information is reported by fraud origin.</p> <p>"Losses due to fraud per liability bearer" are disclosed by a provider reporting fraudulent payment transactions and only with regard to the value of such transactions.</p> | 5a.LF | Number and value of fraudulent transactions – credit transfers, direct debits, cheques |
| | 5a.WF | |
| | 5a.S.LF_PLiW2 | Number and value of fraudulent transactions made with the use of the Issuer's cards and executed by domestic acquirers (by residents) and fraudulent cash withdrawal with the use of a card-based payment instrument of the Issuer settled by domestic acquirers (by residents) |
| | 5a.S.WF_PLiW2 | |
| | 5a.S.LF_krajGEO3 | Number and value of fraudulent transactions made with the use of the Issuer's cards and executed by foreign acquirers (by non-residents) and fraudulent cash withdrawals with the use of the Issuer's executed by foreign acquirers (by non-residents). A breakdown by the country of residence of a foreign acquirer executed card transactions is reported separately in individual tables, i.e. using the following forms: <p>5a.S.L_AT (number of transactions settled by the Austrian acquirer),</p> <p>5a.S.W_AT (value of transactions settled by the Austrian acquirer),</p> <p>5a.S.L_BE (number of transactions settled by the Belgian acquirer),</p> <p>5a.S.W_BE (value of transactions settled by the Belgian acquirer),</p> <p>....,</p> <p>5a.S.L_G1 (number of transactions settled by the acquirer from outside the EEA),</p> <p>5a.S.W_G1 (value of transactions settled by the acquirer from outside the EEA).</p> |
| 5a.S.WF_krajGEO3 | | |
| 5a.S.SF | "Losses due to fraud per liability bearer" collectively for the following transactions: <ol style="list-style-type: none"> credit transfers; direct debits; card-based payment transactions in devices accepting payment cards cash withdrawals using card-based payment instruments; <p>by category: "the reporting PSP", "the payment services user (PSU) of the reporting PSP" and "other".</p> | |
| 5a.R.SF | "Losses due to fraud per liability bearer" collectively for the following transactions: <ol style="list-style-type: none"> card-based payment transactions at ATMs operated by their owners, holders or operators, by category: "the reporting PSP", "the PSU of the reporting PSP" and "other". | |

| | |
|------------------|---|
| 5a.R.LF_PLiW2 | Fraudulent transactions [received] executed at ATMs located in Poland – Number and value of fraudulent card-based transactions executed at ATMs operated by their owners, holders or operators. |
| 5a.R.WF_PLiW2 | |
| 5a.R.LF_krajGEO3 | Number and value of fraudulent card-based transactions executed at ATMs operated by their owners, holders or operators. Transactions received made at ATMs in countries that form part of the EEA and collectively in other countries outside the EEA (so-called GEO3 breakdown). Each country of location of the ATM is reported separately in individual tables, i.e. using the following forms: 5a.R.L_AT (number of transactions in devices on the territory of Austria), 5a.R.W_AT (value of transactions in devices on the territory of Austria), 5a.R.L_BE (number of transactions in devices on the territory of Belgium), 5a.R.W_BE (value of transactions in devices on the territory of Belgium), ..., 5a.R.L_G1 (number of transactions in devices in countries outside the EEA), 5a.R.W_G1 (value of transactions in devices in countries outside the EEA). |
| 5a.R.WF_krajGEO3 | |

The acquirer reports PaySafeCard transactions in the item “E-money payment transactions ” in tables 4a LiW.

Tables in Report AR2 are filled in only for payment card transactions, excluding table 4aLiW.

Reports AR2 and WIP2 are also intended for reporting return/refund transactions with cards, i.e. transactions in which a certain amount of funds is transferred to a card of the holder thereof if the holder returns goods (or parts thereof), after the settlement of the initial purchase transaction paid for by card, usually within few days following the transaction date. Chargeback transactions should not be reported. Reversal transactions should not be reported.

Domestic payment transaction

Domestic payment transaction means “national payment transaction” as defined in Article 2(27) of Regulation (EU) No. 260/2012, i.e. “domestic payment” means a payment transaction initiated by a payer or by a payee, where the payer’s PSP and the payee’s PSP are located in the same member state. For card-based payment transactions, “domestic payment transaction” shall mean “domestic payment transaction” as defined in Article 2(9) of Regulation (EU) 2015/751, i.e. “domestic payment transaction” means any card-based payment transaction which is not a cross-border payment transaction;

Domestic payment transactions are transactions in which the payer’s PSP and the payee’s PSP are resident in the same country. For card-based payment transactions, domestic transactions are payment transactions where the payer’s PSP (issuer) and the payee’s PSP (acquirer) are resident in the same country and where the POS is also resident in that country.



Cross-border payment transaction

A payment transaction initiated by a payer or by a payee, where the payer's PSP (issuer) and the payee's PSP (merchant's acquirer) are located in different countries. For card-based payment transactions, "cross-border payment transaction" shall mean "cross-border payment transaction" as defined in Article 2(8) of Regulation (EU) 2015/751², i.e. "cross-border payment transaction" means a card-based payment transaction where the issuer and the acquirer are located in different member states or where the card-based payment instrument is issued by an issuer located in a member state different from that of the point of sale.

A cross-border payment transaction using card-based payment instruments is a payment transaction where both the issuer and the acquirer are residents in different countries or where the issuer is located in a different country from the POS.

For card-based payment transactions initiated non-remotely, the location of the POS is the location of the physical terminal. For remotely initiated payment transactions, the location of the POS is reported in accordance with the definition of the "point of sale" provided for below.

The location of the terminal (point of sale) indicates the country in which the transaction is made.

The POS terminals are terminals operated by natural persons or unattended terminals (e.g. terminals for paying parking tickets).

Point of sale

POS shall mean, within the meaning of Article 2(29) of Regulation (EU) 2015/751, the address of the physical premises of the merchant at which the payment transaction is initiated. However:

- a) in the case of distance sales or distance contract defined in point 7 of Article 2 of Directive 2011/83/EU, the point of sale shall be the address of the fixed place of business at which the merchant conducts its business, regardless website or server locations through which the payment transaction is initiated;
- b) in the event that the merchant does not have a fixed place of business, the point of sale shall be the address for which the merchant holds a valid business licence through which the payment transaction is initiated;
- c) in the event that the merchant does not have a fixed place of business nor a valid business licence, the point of sale shall be the address for correspondence for the payment of its taxes relating to its sales activity through which the payment transaction is initiated.

² Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions, OJ L 123, 19.5.2015, p. 1–15, <http://data.europa.eu/eli/reg/2015/751/oj>.

An entity that executes payment transactions in the form of credit transfers, direct debits or cheques reports statistical data in the following tables of the WIP2 report: 4a.L, 4a.W, 5a.LF and 5a.WF.

An entity that executes payment card-based payment transactions, reports statistics in the following tables of report WIP2: 4a.S.L_PLiW2, 4a.S.W_PLiW2, 5a.S.LF_PLiW2, 5a.S.WF_PLiW2, 4a.S.L_krajGEO3, 4a.S.W_krajGEO3, 5a.S.LF_GEO3, 5a.S.WF_krajGEO3, 5a.S.SF, 6.c.LiW, 6.ab.LiW, 9.L.MCC, 9.W.MCC, 9.LiW, 4a.R.L_PLiW2, 4a.R.W_PLiW2, 5a.R.LF_PLiW2, 5a.R.WF_PLiW2, 4a.RL_krajGEO3, 4a.RW_krajGEO3, 5a.RLF_GEO3 and 5a.RWF_krajGEO3.

An entity reporting on the side of the ATM’s operator reports statistics in the following tables of report WIP2: 4a.R.L_PLiW2, 4a.R.W_PLiW2, 5a.R.LF_PLiW2, 5a.R.WF_PLiW2, 5a.R.SF, 4a.R.L_krajGEO3, 4a.R.W_krajGEO3, 5a.R.LF_krajGEO3, 5a.RWF_krajGEO3.

An entity reporting on the side of the acquirer reports statistics in the following tables of report AR2: 4a.R.L_PLiW2, 4a.R.W_PLiW2, 5a.R.LF_PLiW2, 5a.R.WF_PLiW2, 5a.R.SF and 4a.R.L_krajGEO3, 4a.R.W_krajGEO3, 5a.R.LF_krajGEO3, 5a.RWF_krajGEO3.

A reporting entity that acts as an acquirer reports statistics for the location of the terminal: POS, Internet website, virtual point of sale, ATM, and next the country of the card issuer.

A reporting entity that acts as a card issuer reports statistics on the side of the acquirer and next of the location of the terminal: POS, Internet website or ATM.

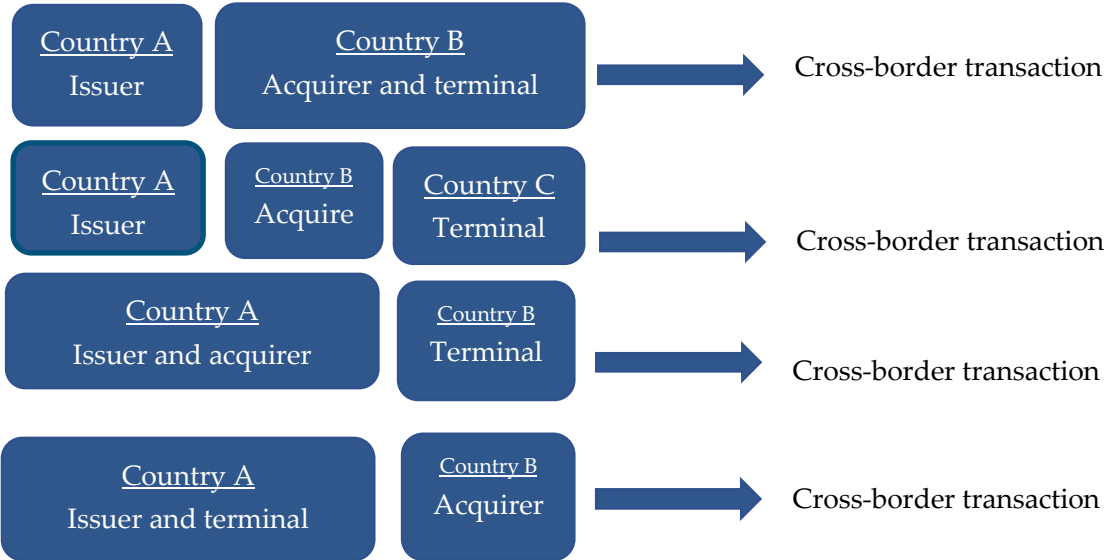
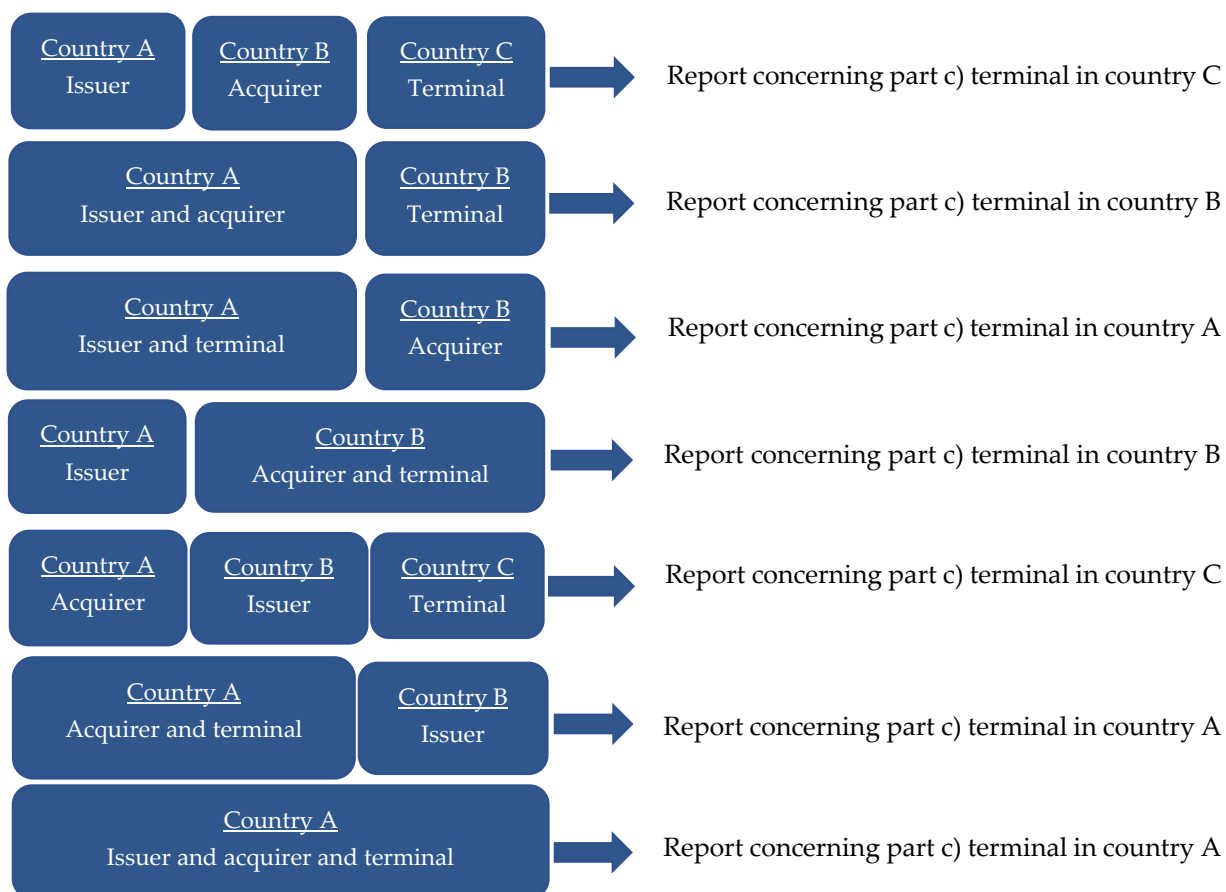


Table 6.c.LiW and table 6.ab.LiW concern only transactions made at physical POS terminals:

- a. transactions at terminals with cards issued by resident PSPs, reported by an acquirer that is a resident;
- b. transactions at terminals with cards issued by non-resident PSPs, reported by an acquirer that is a resident;

c. transactions at terminals, at the location of an acquirer that is not a resident, with cards issued by resident PSPs, reported by an issuer that is a resident.

In Table 6, item “Other transactions at ATMs”, please report transactions made at non-virtual terminals, e.g. phone top-ups at the ATMs and credit transfers. Such operations as a PIN change or balance check are not subject to reporting.



In tables 9.L.MCC, 9.W.MCC, 9.R.L.MCC, 9.R.W.MCC, please report statistics from the following reports:

- AR2 on the side of the country of the card issuer, transactions made at physical POS terminals and Internet websites,
- WIP2 for the location of a terminal: POS, Internet website or ATMs, transactions at physical POS terminals.

2.2. Table 4a

Tables 4a are intended for reporting all transactions (fraudulent and non-fraudulent), and tables 5a for reporting only fraudulent transactions. This means that Table 5a is used for reporting only a subset of transactions reported in table 4a; and in addition Table 5a indicates the fraud origins, which are not specified in Table 4a. For the sake of clarity, Table 4a and Table 5a have the same structure, but in Table 4a the items concerning the origins of fraud are grey/non-coded, which means that such items are not filled in with reporting data, as specified above.

Information reported in Table 4a is compiled in various configurations and is divided into:

- transactions sent and received,
- remote and non-remote transactions,
- payment schemes (e.g. Mastercard, VISA, SEPA and other),
- authentication method applied.

Transaction sent shall mean a transaction involving non-MFIs sent to PSPs. Information is provided in the reporting country by the resident PSP.

For different payment services, the following applies:

- credit transfers are counted on the payer's/debtor's/sender's side
the sending party ("sent") is an entity that sends funds, e.g. the payer's/debtor's bank, and the party receiving ("received") is an entity receiving funds, e.g. the creditor's bank;
- direct debits are counted on the payee's side
the sending party ("sent") is an entity sending a direct debit and simultaneously receiving/obtaining funds, e.g. the creditor's/ funds recipient's bank, and the party receiving ("received") is an entity receiving a direct debit and simultaneously sending the funds, e.g. the payer's/debtor's bank.
- cheques are counted on the payee's side (similarly to the aforementioned direct debits);
- payment card transactions are counted on the payer's, i.e. the issuing, side;
- e-money payment transactions are counted on either the payer's or the payee's side, depending on the initiation channel. If counted on the payer's side under transactions sent, the transaction should be counted on the payee's side under transactions received.

Transaction received shall mean a transaction involving a non-MFIs received from PSPs. Information is provided in the reporting country by the resident PSP.

Remote and non-remote transactions

Credit transfers, card-based payment transactions and e-money payment transactions are further broken down into remote and non-remote payment channels:

- *Remote transaction* shall mean a payment transaction initiated via Internet or a device that can be used as a means of distant communication, a mobile payment (Internet and mobile banking);
- *Non-remote transaction* shall mean a transaction initiated at the ATM, POS terminal, unattended terminal, including with the use of contactless technology, and also in automated payment centres.

SEPA and non-SEPA transactions

Reporting under payment schemes is divided into SEPA schemes and non-SEPA schemes for credit transfers and direct debits. Transactions should be reported separately for each of the schemes, regardless of whether it is a SEPA or a non-SEPA scheme. Pan-European credit transfer schemes include SEPA CT scheme and SEPA CT Inst scheme, and for direct debits pan-European schemes are SEPA DD Core and SEPA DD B2B. Payments in TARGET2 are still counted as non-SEPA payments. The same applies to payments in currencies other than euro, to which SEPA standards are not applicable.

Reasons for authentication via non-Strong Customer Authentication (non-SCA)

Category Other; all payment instruments

Other

Transactions for which the reason for authentication via non-SCA cannot be established.

“Other” is intended for payment card transactions and e-money payment transactions, to which none of the other reasons applies. Examples of such transactions include:

- a card-based payment transaction where the geographical area is cross-border outside the EEA, and a the non-EEA counterparty involved does not support SCA and is not subject to PSD2 requirements (a “one-leg-in” transaction);
- a transaction where additional time is provided for a PSP to migrate to SCA-compliant procedures;
- information on reporting reasons for authentication via non-SCA by the PSP and whether these are reported for remotely (Z)/non-remotely (NZ) initiated transactions:

| | Polecenia przelewu | Wysłana transakcja płatnicza za pomocą karty | Otrzymana transakcja płatnicza za pomocą karty | Transakcja płatnicza pieniądzem elektronicznym |
|---|--------------------|--|--|--|
| Niska wartość | Z | Z | Z | Z |
| Płatność na własną rzecz | Z, NZ | - | - | Z |
| Zaufani odbiorcy | Z, NZ | Z, NZ | - | Z, Nz |
| Transakcja cykliczna | Z, NZ | Z, NZ | Z, NZ | Z, NZ |
| Bezpieczne procesy lub protokoły dotyczące płatności przedsiębiorstw | Z | Z | - | Z |
| Analiza ryzyka transakcji | Z | Z | Z | Z |
| Niskokwotowa wartość zbliżeniowa | NZ | NZ | NZ | NZ |
| Terminale samoobsługowe służące do uiszczania opłat za przejazd i opłat za postój | NZ | NZ | NZ | NZ |
| Inicjowane przez dostawcę świadczącego usługę inicjowania płatności | - | Z | Z | Z |
| Inne | - | Z,NZ | Z,NZ | Z, N |

Innovative payment solutions are reported in accordance with the underlying payment instrument and the initiation channel. For example, if a mobile phone is used exclusively as an initiation/ payment collection channel, such payment transactions should be counted in accordance with the used principal payment service, e.g. a card-based payment transaction, credit transfer, direct debit, etc.

2.2.1. Credit transfer

A credit transfer means a payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the payment service provider which holds the payer's payment account, based on an instruction given by the payer (Directive (EU) 2015/2366 Article 4 (24)).

Credit transfer 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;
- b) payment transactions which take place between two accounts held at the same PSP, e.g. on-us transactions made, 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.

Any transaction in which a credit transfer is initiated at terminal, and a credit card is used for the purpose of authentication of a payment service user (PSU) is not a card-based payment transaction. Any transaction between two customers or between two accounts of the same customer shall be considered the credit transfer (assuming that at least one of the counterparties is a non-monetary institution).

Transactions excluded from credit transfers are transaction orders executed through a simple book entry (simple book entry means a book entry of a loan on the customer's bank account without the use of a traditional payment instrument):

- interest payment by the bank;
- dividend payment by the bank;
- disbursement of the amount of a loan to the current account of the customer;
- other credits to the account by simple book entry.

Credits to the account by simple book entry are not considered as a credit transfer. They may include services related to liquidity management, loan transactions and transactions related to trade in securities. A transaction in which a PSP holding the account only deducts the amount from the customer's payment account is not to be taken into account. Transactions considered an internal bookkeeping operation (intrabank transfers), i.e. operations involving technical accounts within one and the same PSP, outstanding balances of transactions using card-based payment instruments and the movement of funds from direct debit transactions should not be reported.

Rejected credit transfers should not be counted, because they are rejected by the customer bank sphere on the sending side (which does not result in an actual transaction).

As illustrated by the credit transfer sent, Geo 3 geographical breakdown consists of the following elements:

- a) domestic – a credit transfer initiated by a non-MFI is executed from an account with a resident PSP to any other account with the same or other PSP,
- b) breakdown by countries for all EEA countries – a credit transfer initiated by a non-monetary institution is made from an account held by a resident PSP to any other account held by any other PSP which is a non-resident in any of the EEA countries. A separate number is to be reported for each EEA country.
- c) rest of the world – a credit transfer initiated by a non-MFI is executed from an account with a resident PSP to another account with any other PSP which is a resident in a country outside the EEA.

Credit transfers can be divided as follows:

- *Credit transfers initiated in paper-based form*

A credit transfer initiated by a payer in paper-based form or by instructing staff at a branch over the counter (OTC) to initiate a credit transfer and any other credit transfer, which requires manual processing.

- *Credit transfers initiated electronically:*

Credit transfers initiated in a file/batch, and also initiated on a single payment basis, CDs, diskettes.

- Other – credit transfers other than those initiated electronically or in paper-based form: All credit transfers initiated non-electronically and in non-paper-based form, e.g. transactions initiated via mail order or telephone order (MOTO).

Credit transfers initiated in file/batch

An electronically initiated credit transfer that is part of a group of credit transfers jointly initiated by the payer via a dedicated channel. Each credit transfer contained in a batch is counted as a separate credit transfer when reporting the number of transactions.

Credit transfers initiated on a single payment basis

An electronically initiated credit transfer that is initiated independently, i.e. that is not part a group of credit transfers jointly initiated. An individual credit transfer initiated on the basis of a standing order is also reported as initiated on a single payment basis.

Online banking based credit transfers

A credit transfer initiated via online banking and payment initiation services. This includes transactions for which an online banking platform is available via Internet browsers or mobile banking applications. Credit transfers initiated by PISPs via the ASPSP's online banking platform are also included and additionally reported in a dedicated report "Credit transfers initiated by PISPs"; these categories are not mutually exclusive.

E-commerce payments

E-commerce payments made in the form of credit transfers include:

- payments for sale/purchase of goods or services, whether between businesses, households or individuals (pay-by-link).
- electronic transactions conducted via the internet or other computer-mediated (online communication) networks.

The issue covers the ordering of goods and services, via computer networks, but the payment and final delivery of goods or services can be completed both online and offline.

E-commerce payments only include those that are initiated via online banking (“e-commerce payments” is a sub-item of “online banking based credit transfers”). This sub-item does not include e-commerce transactions initiated via other means than those described in the definition of “online banking based credit transfers”. PISP-initiated credit transfers related to e-commerce transactions are also included where they are both initiated using an online banking platform and connected to a purchase on a merchant’s website. Transactions where an ASPSP acts as a PISP to initiate a simple credit transfer for an account at another ASPSP³ are not included. The “e-commerce payments” sub-item corresponds to the “online banking based e-payment” sub-item in Guideline ECB/2014/15 on monetary and financial statistics (the MFS Guideline), i.e. online banking based e-payments – transactions initiated through online banking schemes and payment initiation services. The item “online banking based e-payments” excludes payments merely initiated by the payer via online banking not involving a simultaneous online shopping transaction. It also excludes invoices presented online not involving a simultaneous online shopping transaction.

Transactions with a demand for payment may also be here included if they derive from e-commerce transactions.

ATM or other PSP terminal

Credit transfers at ATMs authenticated by customer using payment cards. These transactions are no longer reported in tables for card transactions. Credit transfers initiated in ATMs or other PSP terminals only include non-remotely initiated payments. Credit transfers initiated at an ATM or other PSP terminal via a mobile payment solution are also reported in this category. Such a credit transfer is not reported as a credit transfer falling in the category of mobile payments (remote).

Transactions at ATMs with a credit transfer function are also reported in this item.

Mobile payment solution

A solution used to initiate payments for which the payments data and the payment instructions are transmitted and/or confirmed via mobile communication and data transmission technology through a mobile device. This category includes digital wallets and other mobile payment solutions used to initiate P2P (person-to-person) and/or C2B (consumer-to-business) transactions, i.e. credit transfers, card payments and/or e-money transactions. For example, BLIK payments of P2P type are included into this category. Transactions initiated at ATMs or other PSP terminals and online banking based credit transfers are excluded. Other operations using BLIK should not be reported under credit transfer category.

³ “E-commerce payments” sub-item corresponds to the “Online banking based e-payments” sub-item in Guideline ECB/2014/15 on monetary and financial statistics (the MFS Guideline), i.e. online banking based e-payments – transactions initiated through online banking schemes and payment initiation services.

P2P mobile payment solution

A solution where payments are initiated, confirmed and/or received by an individual to another individual (P2P), via a mobile device. The payment instruction and other payment data are transmitted and/or confirmed with a mobile device. A distinctive mobile payment identifier, such as mobile telephone number or e-mail address, can be used as a proxy to identify the payer and/or payee. P2P mobile payment solutions can be used to initiate credit transfers, card payments and/or e-money transactions. For example, BLIK payments of P2P type are included in this category. Other operations made using BLIK should not be reported under credit transfer category. . excluded are transactions initiated non-remotely, e.g. at ATMs or other PSP terminals, as well as online banking based credit transfers. Requests for BLIK payments should not be reported, only BLIK transactions.

Credit transfers are broken down into:

- remote payment channels: online banking transfers or mobile payments;
- non-remote payment channels: transfers initiated via ATMs or other terminals. Transactions at terminals, including using contactless technology.

Payment schemes

- SEPA CT scheme,
- SEPA CT inst scheme,
- via non-scheme credit transfers: the item should include transactions executed in payment schemes in which SEPA standard was not used and transactions transferred via a correspondent bank,
- on-us credit transfers and inter-branch credit transfers.

Authentication

Authentication means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials (pursuant to Article 4 (29) of Directive (EU) 2015/2366).

Strong customer authentication (SCA)

Strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data (Article 4 (30) of Directive (EU) 2015/2366).

Pursuant to Article 97 (1) of PSD2, “(...) a payment service provider applies strong customer authentication where the payer:

- a) accesses its payment account online;
- b) initiates an electronic payment transaction;
- c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.”.

These requirements should not apply jointly, i.e. the SCA system applies when at least one of them is met.

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

Authenticated via non-strong customer authentication refers to transactions which are exempted from strong customer authentication pursuant to Chapter III of Commission Delegated Regulation (EU) 2018/389 as well as transactions for which the provisions of Article 97(1) of Directive (EU) 2015/2366 do not apply. Merchant initiated transactions as well as other transactions to which SCA is not applicable are included.

Reasons for authentication via non-strong customer authentication (non-SCA)

Low value

Payment transactions for which the exemption in Article 16 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the amount of the remote electronic payment transaction does not exceed EUR 30;
- 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;
- 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. The individual amount of the contactless electronic payment transaction does not exceed EUR 50.

Payment to self

Payment transactions for which the exception in Article 15 of the Commission Delegated Regulation (EU) 2018/389 applies: 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. These payments can be credit transfers and e-money transactions.

Trusted beneficiaries

Payment transactions for which the exception in Article 13 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider,
- the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.

Recurring transaction

Payment transactions for which the exception in Article 14 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee,
- payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions referred above.

Secure corporate payment processes and protocols

Payment transactions for which the exception in Article 17 of the Commission Delegated Regulation (EU) 2018/389 applies: Payment service providers shall be allowed not to apply strong customer authentication, 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 for by Directive (EU) 2015/2366.

Transaction risk analysis

Payment transactions for which the exception in Article 18 of the Commission Delegated Regulation (EU) 2018/389 applies, that is:

1. Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.
2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:

- a) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Annex for “remote electronic card-based payments” and “remote electronic credit transfers” respectively;
- b) the amount of the transaction does not exceed the relevant exemption threshold value (‘ETV’) specified in the table set out in the Annex;
- c) payment service providers as a result of performing a real time risk analysis have not identified any of the following:
 - (i) abnormal spending or behavioural pattern of the payer;
 - (ii) unusual information about the payer's device/software access;
 - (iii) malware infection in any session of the authentication procedure;
 - (iv) known fraud scenario in the provision of payment services;
 - (v) abnormal location of the payer;
 - (vi) high-risk location of the payee.

3. Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

- a) the previous spending patterns of the individual payment service user;
- b) the payment transaction history of each of the payment service provider's payment service users;
- c) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;
- d) the identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.

Contactless low value

- Contactless payment transactions to which the exception in Article 11 of the Commission Delegated Regulation (EU) 2018/389 applies: the individual amount of the contactless electronic payment transaction does not exceed EUR 50;
- 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;

- 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

This applies to bank transfers, card-based payment transactions and e-money payment transactions.

Unattended terminals for transport fares or parking fees

Payment transactions for which the exception in Article 12 of the Commission Delegated Regulation (EU) 2018/389 applies: the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

2.2.2. Direct debit

A direct debit means a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider (Article 4 (23) of Directive (EU) 2015/2366).

Direct debits are initiated by a payee (e.g. a public utility company) on the basis of a mandate given by a payer. Both recurring and one-off direct debits are included. In the case of recurring direct debits, each individual direct debit payment is counted as one payment transaction. Direct debits used to settle outstanding balances resulting from payment transactions using credit card or delayed debit card are also included.

Direct debits rejected due to insufficient funds must also be reported, because they are rejected in an interbank zone on the recipient side (in which case the actual transaction is made, and subsequently rejected).

Direct debit initiated in a file/batch

An electronically initiated direct debit that is part of a group of direct debits initiated jointly by the payee. Each direct debit contained in a batch is counted as a separate direct debit.

Direct debit initiated on a single payment basis

An electronically initiated direct debit that is independent from other direct debits, i.e. that is not part of a group of direct debits jointly initiated.

Consent given via an electronic mandate

"Mandate" means the expression of consent and authorisation given by the payer to the payee and (directly or indirectly via the payee) to the payer's PSP to allow the payee to initiate a collection for

debiting the payer's specified payment account and to allow the payer's PSP to comply with such instructions, as defined in Article 2 (21) of Regulation EU No. 260/2012.

Mandate given in other form

Direct debits to which the payer has given consent in non-electronic form. Direct debits where the PSP is not involved in providing the mandate and where the PSP is also not able to obtain any information on the form of the consent.

Payment schemes

- SEPA CT scheme,
- SEPA CT Inst scheme,
- via non-scheme direct debits: this item should include transactions executed in payment schemes in which SEPA standard was not used and transactions transferred via a correspondent bank,
- via on-us direct debits and inter-branch direct debits.

2.2.3. Card-based payment transactions

A card-based payment transaction means a service based on a payment card scheme's infrastructure and business rules to make a payment transaction by means of any card, telecommunication, digital or IT device or software if this results in a debit or a credit card transaction. Card-based payment transactions exclude transactions based on other kinds of payment services, in accordance with Article 2 (7) of Regulation (EU) No. 751/2015, including a delayed debit card.

Card-based payment instrument

Pursuant to Article 2 (20) of Regulation (EU) No. 751/2015, a card-based payment instrument means any payment instrument, including a card, mobile phone, computer or any other technological device containing the appropriate payment application which enables the payer to initiate a card-based payment transaction which is not a credit transfer or a direct debit as defined by Article 2 of Regulation (EU) No 260/2012, including a delayed debit card.

Acquirer

Pursuant to Article 2 (1) of Regulation EU No. 751/2015, an acquirer means a payment service provider contracting with a payee to accept and process card-based payment transactions, which result in a transfer of funds to the payee.

Card issuer

Pursuant to Article 2 (2) of Regulation (EU) No. 751/2015, a card issuer means a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer's card-based payment transactions.

Acquiring of payment transactions

Pursuant to Article 4 (44) of Directive (EU) 2366/2015, acquiring of payment transactions means a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee.

Initiated electronically

Card-based payment transactions which are initiated in POS, ATM or any other physical terminal that allows electronic payment initiation or payment transactions initiated online (via the Internet).

Initiated non-electronically

Card-based payment transactions initiated at a physical terminal through a manual authorisation procedure (e.g. imprinters), authenticated with a signature placed at the POS, either on paper or by means of mail order or telephone order (MOTO)(card not present transactions (CNP)).

Mobile payment solution

A solution used to initiate payments for which the payments data and the payment instructions are transmitted and/or confirmed via mobile communication and data transmission technology through a mobile device. This category includes digital wallets and other mobile payment solutions used to initiate P2P (person-to-person) and/or C2B (consumer-to-business) transactions, i.e. credit transfers, card payments and/or e-money transactions.

P2P mobile payment solution

A solution where payments are initiated, confirmed and/or received by an individual to another individual (P2P), via a mobile device. A distinctive mobile payment identifier, such as mobile telephone number or e-mail address, can be used as a proxy to identify the payer and/or payee. P2P mobile payment solutions can be used to initiate credit transfers, card payments and/or e-money transactions. For cards, phone-to-phone transactions between individual users must be reported, e.g. a card-based mobile payment using a digital wallet in a physical shop (C2B):

- included in the payment cards/ mobile payments category

- not included in the payment cards/ mobile payments / of which: P2P mobile payment category.

Contactless payment

A payment transaction using a card or other means where the payer and merchant (and/or their equipment) are at the same physical location and where the communication between the portable device and the POS terminal takes place through contactless technology.

NFC payments

This category includes contactless payments with cards and/or portable devices using NFC technology (e.g. mobile payments initiated via mobile card-based wallets). A contactless payment transaction using near-field communication (NFC) technology (ISO/ IEC 18092).

Strong customer authentication (SCA)

Strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data (Article 4 (30) of Directive (EU) 2015/2366).

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

Authenticated via non-strong customer authentication refers to transactions which are exempted from strong customer authentication pursuant to Chapter III of Commission Delegated Regulation (EU) 2018/389, as well as transactions for which the provisions in Article 97(1) of Directive (EU) 2015/2366 do not apply. Merchant initiated transactions as well as other transactions to which SCA is not applicable are included.

Reasons for authentication via non-strong customer authentication (non-SCA)

Trusted beneficiaries

Payment transactions for which the exception in Article 13 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider,
- the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.

Recurring transaction

Payment transactions for which the exception in Article 14 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee,
- payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions referred above.

Contactless low value

- Contactless payment transactions for which the exception in Article 11 of the Commission Delegated Regulation (EU) 2018/389 applies: the individual amount of the contactless electronic payment transaction does not exceed EUR 50;
- 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;
- 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.

This applies to bank transfers, card-based payment transactions and e-money transactions.

Unattended terminals for transport fares or parking fees

Payment transactions for which the exception in Article 12 of the Commission Delegated Regulation (EU) 2018/389 applies: the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

Low value

Payment transactions for which the exception in Article 16 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the amount of the remote electronic payment transaction does not exceed EUR 30;
- 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;
- 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. The individual amount of the contactless electronic payment transaction does not exceed EUR 50.

Secure corporate payment processes and protocols

Payment transactions for which of the exception in Article 17 of the Commission Delegated Regulation (EU) 2018/389 applies: Payment service providers shall be allowed not to apply strong customer authentication, 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 for by Directive (EU) 2015/2366.

Transaction risk analysis

Payment transactions for which the exception in Article 18 of the Commission Delegated Regulation (EU) 2018/389 applies, that is:

1. Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article;
2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:
 - a) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Annex for “remote electronic card-based payments” and “remote electronic credit transfers” respectively;
 - b) the amount of the transaction does not exceed the relevant exemption threshold value (‘ETV’) specified in the table set out in the Annex;
 - c) payment service providers as a result of performing a real time risk analysis have not identified any of the following:
 - (i) abnormal spending or behavioural pattern of the payer;
 - (ii) unusual information about the payer's device/software access;
 - (iii) malware infection in any session of the authentication procedure;
 - (iv) known fraud scenario in the provision of payment services;
 - (v) abnormal location of the payer;
 - (vi) high-risk location of the payee.

3. Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

- a) the previous spending patterns of the individual payment service user;
- b) the payment transaction history of each of the payment service provider's payment service users;
- c) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;
- d) the identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.

Merchant initiated transaction

Merchant initiated transaction means “Merchant initiated transaction” as defined in Annex II Part C footnote 4 of the EBA Guidelines amending the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) of Directive (EU) 2015/2366 (EBA/GL/2020/01), i.e.: card-based payment transactions that meet conditions specified by the European Commission in Q&A 2018_4131 and Q&A 2018_4031, and which therefore are considered transactions initiated by the payee and not subject to the obligation to apply strong customer authentication referred to in Article 97 of the Payment Services Directive (PSD2).

Cash withdrawals using card-based payment instruments

Cash withdrawals at ATMs or at banks' counters or at POS terminals using payment card with a cash function.

2.2.4. Cheques

A written and signed order from one party, i.e. the drawer, to another, i.e. the drawee, which is in principle a credit institution, requiring the drawee to pay a specified sum unconditionally and on demand to the drawer or to a third party specified by the drawer.

Categories include cheques issued and submitted for payment:

1. The “sent cheques” sub-category is counted from the payee's side. For domestic cheques, the PSPs of both parties (the payer and the payee) are resident in the reporting country. For cross-border transactions, the payee submits a cheque to a PSP resident in the reporting country, while the PSP of the payer is resident outside the country.

2. The “received cheques” sub-category is counted from the payer’s side. For domestic cheques, the PSPs of both parties (the payer and the payee) are resident in the reporting country. For cross-border transactions, the PSP of the payer is resident in the reporting country, while the PSP of the payee is resident outside the country.

Cash withdrawals using cheques, cash withdrawals using a bank form, cheques issued but not submitted for clearing are not included.

2.2.5. E-money payment transactions WPE2/WIPE2

An electronic money transaction means a payment transaction using “electronic money”, as defined in Article 2 (2) of Directive 2009/110/EC, i.e. “electronic money” means 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 2007/64/EC, (“payment transaction” means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee) and which is accepted by a natural or legal person other than the electronic money issuer.

E-money payment transactions are counted as either sent or received according to the initiation side; in particular, if initiated by the payee they are counted as received from the payer’s side.

E-money account

An account on which e-money is stored and in which the balance that can be used by the account holder to make payments and to transfer funds between accounts.

E-money cards

A card on which e-money can be stored directly or cards which give access to e-money stored on e-money accounts, enabling payment transactions using e-money.

Virtual cards are not reported as e-money cards. Only prepaid virtual cards are included. Coupons, gift vouchers that are only accepted by a limited number of merchants are excluded from the reporting of e-money cards on which e-money can be stored directly.

Monetary value stored on specific prepaid instruments does not represent electronic money if the instruments allow the electronic money holder to purchase goods or services only on the premises of the electronic money issuer or within a limited network of service providers under a direct commercial agreement with a professional issuer, or they can only be used to acquire a limited range of goods or services. Such instruments may include: store cards, petrol cards, membership cards, public transport cards, meal vouchers or vouchers for services. These cards and transaction with these cards are not included in the reporting for payments statistics.

E-money account accessed through a card

In accordance with the definition of “e-money account” and “card with an e-money function”.

E-money payment with cards on which e-money can be stored directly

A transaction whereby the holder of a card with e-money function transfers e-money value from its balance stored on the card to the balance of the beneficiary.

E-money payment transactions with e-money issued by resident PSPs [sent] with e-money accounts

A transaction whereby funds are transferred from an e-money account of a payer to the account of a payee.

E-money payment transactions with e-money issued by resident PSPs [sent] with e-money accounts, of which accessed through a card

A transaction in which a card is used in order to gain access to an electronic money account, and in which next funds are transferred from the payer’s electronic money account to the payee’s account.

Mobile payment solution

A solution used to initiate payments for which the payments data and the payment instructions are transmitted and/or confirmed via a mobile communication and data transmission technology through a mobile device. This category includes digital wallets and other mobile payment solutions used to initiate P2P (person-to-person) and/or C2B (consumer-to-business) transactions, i.e. credit transfers, card payments and e-money transactions.

P2P mobile payment solution

A solution where payments are initiated, confirmed and/or received by an individual to another individual (P2P), via a mobile device. The payment instruction and other payment data are transmitted and/or confirmed with a mobile device. A distinctive mobile payment identifier, such as mobile telephone or e-mail address, can be used as a proxy to identify the payer and/or payee. P2P mobile payment solutions can be used to initiate credit transfers, card payments or e-money transactions.

Strong customer authentication (SCA)

Strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one

does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data (Article 4 (30) of Directive (EU) 2015/2366).

Authenticated via non-Strong Customer Authentication (non-SCA)

Authenticated via non-strong customer authentication refers to transactions which are exempted from strong customer authentication pursuant to Chapter III of Commission Delegated Regulation (EU) 2018/389 as well as transactions for which the provisions of Article 97(1) of Directive (EU) 2015/2366 do not apply. Merchant initiated transactions as well as other transactions to which SCA is not applicable are included.

Reasons for authentication via non-strong customer authentication (non-SCA)

Low value

Payment transactions for which the exception in Article 16 of the Commission Delegated Regulation (EU) 2018/389 applies:

Payment service providers are not obliged to apply strong customer authentication if payee initiates remote electronic payment transaction and if 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.

Trusted beneficiaries

Payment transactions for which the exception in Article 13 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider,
- the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.

Recurring transactions

Payment transactions for which the exception in Article 14 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee,
- payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions referred above.

Payments to self

Payment transactions for which the exception in Article 15 of the Commission Delegated Regulation (EU) 2018/389 applies: 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. These payments can be credit transfers and e-money transactions.

Secure corporate payment processes and protocols

Payment transactions for which the exception in Article 17 of the Commission Delegated Regulation (EU) 2018/389 applies: Payment service providers shall be allowed not to apply strong customer authentication, 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 for by Directive (EU) 2015/2366.

Transaction risk analysis

Payment transactions for which the exception in Article 18 of the Commission Delegated Regulation (EU) 2018/389 applies, that is:

1. Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.
2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:
 - a) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Annex for “remote electronic card-based payments” and “remote electronic credit transfers” respectively;
 - b) the amount of the transaction does not exceed the relevant exemption threshold value (‘ETV’) specified in the table set out in the Annex;

c) payment service providers as a result of performing a real time risk analysis have not identified any of the following:

- (i) abnormal spending or behavioural pattern of the payer;
- (ii) unusual information about the payer's device/software access;
- (iii) malware infection in any session of the authentication procedure;
- (iv) known fraud scenario in the provision of payment services;
- (v) abnormal location of the payer;
- (vi) high-risk location of the payee.

3. Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

- a) the previous spending patterns of the individual payment service user;
- b) the payment transaction history of each of the payment service provider's payment service users;
- c) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;
- d) the identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.

Contactless low value

- Contactless payment transactions for which the exception in Article 11 of the Commission Delegated Regulation (EU) 2018/389 applies: the individual amount of the contactless electronic payment transaction does not exceed EUR 50;
- 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;
- 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.

This applies to bank transfers, card-based payment transactions and e-money transactions.

Unattended terminals for transport fares or parking fees

Payment transactions for which the exception in Article 12 of the Commission Delegated Regulation (EU) 2018/389 applies: the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

Merchant initiated transaction

Merchant initiated transaction means “Merchant initiated transaction” as defined in Annex II Part C footnote 4 of the EBA Guidelines amending the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) of Directive (EU) 2015/2366 (EBA/GL/2020/01), i.e.: card-based payment transactions that meet conditions specified by the European Commission in Q&A 2018_4131 and Q&A 2018_4031, and which therefore are considered transactions initiated by the payee and not subject to the obligation to apply strong customer authentication referred to in Article 97 of the Payment Services Directive (PSD2) (PSD2).

2.3. Tables 5

Tables 4a are intended for reporting all transactions (fraudulent and non-fraudulent), and tables 5a for reporting only fraudulent transactions. This means that Table 5a is used for reporting only a subset of transactions reported in Table 4a; and in addition Table 5a indicates fraud origins, which are not specified in Table 4a. For the sake of clarity, Table 4a and Table 5a have the same structure, but in Table 4a the items concerning the origins of fraud are grey/non-coded, which means that such items are not filled in with reporting data, as specified above.

Fraudulent payment transaction

A fraudulent payment transaction includes all instances of payment fraud referred to in Guideline 1.1 of the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) PSD2 (EBA/GL/2018/05), i.e.:

- a) unauthorised payment transactions made, including as a result of 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 (“unauthorised payment transactions”); and
- b) payment transactions made as a result of the payer being manipulated by the fraudster 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 (“manipulation of the payer”).

Fraudulent payment transactions are reported in the dedicated tables on fraud (5a... for WIP2). Transactions to be reported include all transactions:

- reported as fraudulent, and not only confirmed frauds or transactions recognised as fraudulent by you;
- detected as fraudulent.

A transaction is reported in a quarter in which it was made and not in a quarter in which it was detected. If a fraudulent transaction was made in Q1 2022 and reported in Q2 2022, a corrected report, including information on the detected fraudulent transaction shall be submitted for Q1 2022. The date of transaction is decisive.

If it turns out that the reported transaction is not fraudulent, a corrected report shall be submitted and the transaction concerned shall be excluded from the statistics for a given quarter.

2.3.1. Credit transfer

Strong customer authentication (SCA)

Strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data (Article 4 (30) of Directive (EU) 2015/2366).

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

Authenticated via non-strong customer authentication refers to transactions which are exempted from strong customer authentication pursuant to Chapter III of Commission Delegated Regulation (EU) 2018/389 as well as transactions for which provisions in Article 97(1) of Directive (EU) 2015/2366 do not apply. Merchant initiated transactions as well as other transactions to which SCA is not applicable are included.

Issuance of a payment order by the fraudster

It is a type of unauthorised payment transaction, as defined in the Guideline 1.1.(a) of the EBA Guidelines on reporting requirements for fraud data under Article 96(6) PSD2: *a) unauthorised payment transactions made, including as a result of 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 (“unauthorised payment transactions”)* and refers to a situation where a fake payment order is issued by the fraudster after having obtained the payer/payee's sensitive payment data through fraudulent means.

Modification of a payment order by the fraudster

This means “modification of a payment order by the fraudster” within the meaning of the Guideline 1.6 (c) of the EBA Guidelines on reporting requirements for fraud data under Article 96(6) PSD2 (EBA/GL/2018/05), i.e.: it is a type of unauthorised transaction as defined in Guideline 1.1(a) and refers to a situation 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 (for instance through malware or attacks allowing attackers to eavesdrop on the communication between two legitimately communicating hosts (man-in-the middle attacks)) or modifies the payment instruction in the payment service provider’s system before the payment order is cleared and settled.

Reasons for authentication via non-Strong Customer Authentication (non-SCA)

Low value

Payment transactions for which the exception in Article 16 of the Commission Delegated Regulation (EU) 2018/389 applies:

Payment service providers are not obliged to apply strong customer authentication if payee initiates remote electronic payment transaction and if 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.

Payments to self

Payment transactions for which the exception in Article 15 of the Commission Delegated Regulation (EU) 2018/389 applies: 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. These payments can be credit transfers and e-money transactions.

Trusted beneficiaries

Payment transactions for which the exception in Article 13 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider,

- the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.

Recurring transaction

Payment transactions for which the exception in Article 14 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee,
- payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions referred above.

Secure corporate payment processes and protocols

Payment transactions for which the exception in Article 17 of the Commission Delegated Regulation (EU) 2018/389 applies: Payment service providers shall be allowed not to apply strong customer authentication, 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 for by Directive (EU) 2015/2366.

Transaction risk analysis

Payment transactions for which the exception in Article 18 of the Commission Delegated Regulation (EU) 2018/389 applies, that is:

1. Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.
2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:
 - a) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Annex for “remote electronic card-based payments” and “remote electronic credit transfers” respectively;
 - b) the amount of the transaction does not exceed the relevant exemption threshold value (‘ETV’) specified in the table set out in the Annex;

c) payment service providers as a result of performing a real time risk analysis have not identified any of the following:

- (i) abnormal spending or behavioural pattern of the payer;
- (ii) unusual information about the payer's device/software access;
- (iii) malware infection in any session of the authentication procedure;
- (iv) known fraud scenario in the provision of payment services;
- (v) abnormal location of the payer;
- (vi) high-risk location of the payee.

3. Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

- a) the previous spending patterns of the individual payment service user;
- b) the payment transaction history of each of the payment service provider's payment service users;
- c) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;
- d) the identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.

Contactless low value

- Contactless payment transactions for which the exception in Article 11 of the Commission Delegated Regulation (EU) 2018/389 applies: the individual amount of the contactless electronic payment transaction does not exceed EUR 50;
- 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;
- 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.

This applies to bank transfers, card-based payment transactions and e-money transactions.

Unattended terminals for transport fares or parking fees

Payment transactions for which the exception in Article 12 of the Commission Delegated Regulation (EU) 2018/389 applies: the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

Initiated by PISP

The item is reported by an account servicing payment service provider (ASPSP), Reporting agents, in their capacity as ASPSPs, should include payments initiated by third party PISPs on behalf of payers that have payment accounts with that particular reporting PSP.

2.3.2. Direct debit

Consent given via an electronic mandate

“Mandate” means the expression of consent and authorisation given by a payer to a payee and (directly or indirectly via the payee) to the payer’s PSP to allow the payee to initiate a collection for debiting the payer’s specified payment account and to allow the payer’s PSP to comply with such instructions, as defined in Article 2 (21) of Regulation (EU) No. 260/2012.

Mandate given in other form

Direct debits to which the payer has given consent in non-electronic form. Direct debits where the PSP is not involved in providing the mandate and where the PSP is also not able to obtain any information on the form of the consent.

Unauthorised payment transaction

within the meaning of guideline 1.1 (a) of the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) PSD2 (EBA/GL/2018/05), i.e.: unauthorised payment transactions made, including as a result of 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.

Manipulation of the payer

payment transactions made as a result of the payer being manipulated by the fraudster 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.

Losses due to fraud per liability bearer

within the meaning of Guideline 1.6 (b) of the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) oPSD2 (EBA/GL/2018/05), i.e.: 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.

2.3.3. Card-based payment transactions

Strong customer authentication (SCA)

Strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data (Article 4 (30) of Directive (EU) 2015/2366).

Authenticated via non-Strong Customer Authentication (non-SCA)

Authenticated via non-strong customer authentication refers to transactions which are exempted from strong customer authentication pursuant to Chapter III of Commission Delegated Regulation (EU) 2018/389 as well as transactions for which provisions in Article 97(1) of Directive (EU) 2015/2366 do not apply. Merchant initiated transactions as well as other transactions to which SCA is not applicable are included.

Issuance of a payment order by the fraudster

This is an unauthorised payment transaction, as defined in the guideline 1.1. (a) of the EBA Guidelines on reporting requirements for fraud data under Article 96(6) PSD2: *a) unauthorised payment transactions made, including as a result of 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 ("unauthorised payment transactions")* and refers to a situation where a fake payment order is issued by the fraudster after having obtained the payer/payee's sensitive payment data through fraudulent means.

Modification of a payment order by the fraudster

This mean "modification of a payment order by the fraudster" within the meaning of the Guideline 1.6 (c) of the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) PSD2 (EBA/GL/2018/05), i.e.: is a type of unauthorised transaction as defined in Guideline 1.1(a) and

refers to a situation 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 (for instance through malware or attacks allowing attackers to eavesdrop on the communication between two legitimately communicating hosts (man-in-the middle attacks)) or modifies the payment instruction in the payment service provider's system before the payment order is cleared and settled.

Lost or stolen card

A fraud type that occurs with the use of a lost or stolen card-based payment instrument (debit card, delayed debit or credit card) without the actual, implied or apparent authority of the cardholder.

Card not received

A card-based payment instrument 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

The use of an altered or illegally reproduced card-based payment instrument, including the replication or alteration of the magnetic strip or embossing.

Card details theft

Theft of sensitive payment data within the meaning of Article 4 (32) of Directive (EU) 2015/2366. Sensitive payment data in this case refer to data on a card-based payment instrument, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data.

Reasons for authentication via non-Strong Customer Authentication (non-SCA)

Trusted beneficiaries

Payment transactions for which the exception in Article 13 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider,
- the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.

Recurring transaction

Payment transactions for which the exception in Article 14 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee,
- payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions referred above.

Contactless low value

- Contactless payment transactions for which the exception in Article 11 of the Commission Delegated Regulation (EU) 2018/389 applies: the individual amount of the contactless electronic payment transaction does not exceed EUR 50;
- 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;
- 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.

This applies to bank transfers, card-based payment transactions and e-money transactions.

Unattended terminals for transport fares or parking fees

Payment transactions for which the exception in Article 12 of the Commission Delegated Regulation (EU) 2018/389 applies: the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

Low value

Payment transactions for which the exception in Article 16 of the Commission Delegated Regulation (EU) 2018/389 applies:

Payment service providers are not obliged to apply strong customer authentication if payee initiates remote electronic payment transaction and if 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.

Secure corporate payment processes and protocols

Payment transactions for which the exception in Article 17 of the Commission Delegated Regulation (EU) 2018/389 applies: Payment service providers shall be allowed not to apply strong customer authentication, 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 for by Directive (EU) 2015/2366.

Transaction risk analysis

Payment transactions for which of the exception in Article 18 of the Commission Delegated Regulation (EU) 2018/389 applies, that is:

1. Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.

2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:

a) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Annex for “remote electronic card-based payments” and “remote electronic credit transfers” respectively;

b) the amount of the transaction does not exceed the relevant exemption threshold value (‘ETV’) specified in the table set out in the Annex;

c) payment service providers as a result of performing a real time risk analysis have not identified any of the following:

(i) abnormal spending or behavioural pattern of the payer;

(ii) unusual information about the payer's device/software access;

(iii) malware infection in any session of the authentication procedure;

(iv) known fraud scenario in the provision of payment services;

(v) abnormal location of the payer;

(vi) high-risk location of the payee.

3. Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

- a) the previous spending patterns of the individual payment service user;
- b) the payment transaction history of each of the payment service provider's payment service users;
- c) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;
- d) the identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.

Merchant initiated transaction

Merchant initiated transaction means “Merchant initiated transaction” as defined in Annex II Part C footnote 4 of the EBA Guidelines amending the EBA Guidelines on reporting requirements for fraud data under Article 96(6) of the Payment Services Directive (EU) 2015/2366 (EBA/GL/2020/01), i.e.: card-based payment transactions that meet conditions specified by the European Commission in Q&A 2018_4131 and Q&A 2018_4031, and which therefore are considered transactions initiated by the payee and not subject to the obligation to apply strong customer authentication referred to in Article 97 of the Payment Services Directive (PSD2).

Losses due to fraud per liability bearer

within the meaning of Guideline 1.6(b) of the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) PSD2 (EBA/GL/2018/05), i.e.: 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.

2.3.4. Cash withdrawal

Cash withdrawals using card-based payment instruments (excluding e-money transactions).

Cash withdrawal at an ATM or the counter of a PSP using a card with a cash function. E-money payment transactions are not included while cash advances at POS terminals are included.

Issuance of a payment order by the fraudster

This is an unauthorised payment transaction, as defined in the Guideline 1.1(a) of the EBA Guidelines on reporting requirements for fraud data under Article 96(6) PSD2: *a) unauthorised payment transactions made, including as a result of 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 (“unauthorised payment transactions”)* and refers to a situation where a fake payment order is issued by the fraudster after having obtained the payer/payee's sensitive payment data through fraudulent means.

Lost or stolen card

A fraud type that occurs with the use of a lost or stolen card-based payment instrument (debit card, delayed debit or credit card) without the actual, implied or apparent authority of the cardholder.

Card not received

A card-based payment instrument that the payer claimed was received, although the payer's PSP (issuer) confirms it was sent to the payer (by any delivery method).

Counterfeit card

The use of an altered or illegally reproduced card-based payment instrument, including the replication or alteration of the magnetic strip or embossing.

Losses due to fraud per liability bearer

within the meaning of guideline 1.6(b) of the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) PSD2 (EBA/GL/2018/05), i.e.: 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.

2.4. General information on filling in WPE2/WIPE2 forms

“**Electronic Money**” means electronically, including magnetically, stored monetary value, which is issued, with the obligation of its redemption, on receipt of funds for the purpose of making payment transactions, accepted by entities other than only the electronic money issuer (APS, Article 2(21a)); the activity in the scope of electronic money issuing and its redemption may be performed only by electronic money issuers (APS, Article 4(2a)); electronic money issuers may include the following entities (APS, Article 4(2)(1-4) and (6-8)):

- a domestic bank within the meaning of Article 4(1)(1) of the Banking Act;
- a branch of a foreign bank within the meaning of Article 4(1)(20) of the Banking Act;
- a credit institution within the meaning of Article 4(1)(17) of the Banking Act and, respectively, a branch of a credit institution within the meaning of Article 4(1)(18) of the Banking Act;
- an electronic money institution;
- a payment institution;
- the European Central Bank, Narodowy Bank Polski and the central bank of another Member State – other than acting in their capacity as monetary authorities or public administration bodies;
- a public administration body
and (APS, Article 4 (2b)):
- a branch of a foreign electronic money institution;
- a branch of an entity providing postal payment services in the Member State other than the Republic of Poland, authorised in compliance with the law of such a state to issue electronic money and Poczta Polska Spółka Akcyjna to the extent the provision of Article 13(1)(2a) of the Act of 5 September 2008 on commercialisation of a state enterprise of public utility “Poczta Polska” (Journal of Laws No. 180 item 1109, of 2012 item 1529 and of 2013 item 1036) authorises it to issue electronic money;
- a credit union.

Funds received by payment institutions, payment service offices, electronic money institutions and branches of foreign electronic money institutions in connection with the provision of payment services and in return for the electronic money issued shall not constitute a deposit or other refundable funding within the meaning of Article 726 of the Act of 23 April 1964 – the Civil Code (Article 7(1) of the APS).

In WIPE2 form statistical information is provided to NBP by the issuer of the payment instrument on which e-money issued by another entity is stored. In this case, the issuer of the payment instrument is not the issuer of e-money. If the issuer of the payment instrument is at the same time the issuer of e-money, it shall report statistical information on e-money under the WIP2 form addressed to electronic money issuers.

The funds received in return for the electronic money issued shall not bear interest or generate for the electronic money holder any other benefits dependent on the period of holding electronic money (Article 7(4) of the APS).

The guidance concerning the way of defining electronic money is contained in the following recitals of the Preamble to Directive of the European Parliament and of the Council 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC:

“(5) It is appropriate to limit the application of this Directive to payment service providers that issue electronic money. This Directive should not apply to monetary value held 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.

An instrument should be considered to be used within such a limited network if it can be used only either for the purchase of goods and services in a specific store or chain of stores, or for a limited range of goods or services, regardless of the geographical location of the point of sale.

Such instruments could include store cards, petrol cards, membership cards, public transport cards, meal vouchers or vouchers for services (such as vouchers for childcare, or vouchers for social or services schemes which subsidise the employment of staff to carry out household tasks such as cleaning, ironing or gardening) (...). Where such a specific-purpose instrument develops into a general-purpose instrument, the exemption from the scope of this Directive should no longer apply.

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.

(6) 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.

(7) It is appropriate to introduce a clear definition of electronic money in order to make it technically neutral. That definition should cover all situations where the payment service provider issues a pre-paid stored value in exchange for funds, which can be used for payment purposes because it is accepted by third persons as a payment.

(8) The definition of electronic money should cover electronic money whether it is held on a payment device in the electronic money holder's possession or stored remotely at a server and managed by the electronic money holder through a specific account for electronic money. That definition should be wide enough to avoid hampering technological innovation and to cover not only all the electronic money products available today in the market but also those products which could be developed in the future.

(18) Electronic money needs to be redeemable to preserve the confidence of the electronic money holder. Redeemability does not imply that the funds received in exchange for electronic money should be regarded as deposits or other repayable funds for the purpose of Directive 2006/48/EC. Redemption should be possible at any time, at par value without any possibility to agree a minimum threshold for redemption. Redemption should, in general, be granted free of charge. (...). "

An e-money payment transaction means a payment transaction using "electronic money", as defined in Article 2 (2) of Directive 2009/110/EC, i.e. "electronic money" means 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 2007/64/EC, ("payment transaction" means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee) and which is accepted by a natural or legal person other than the electronic money issuer.

E-money payment transactions are counted as sent or received depending on the initiating party; if they are initiated by the payee, they are counted as received on the payer's side.

Cards with an e-money function:

A card on which e-money can be stored directly and/or which gives access to e-money stored on e-money accounts, enabling e-money payment transactions.

This card can be a *card on which e-money can be stored* or a *card which gives access to e-money stored on e-money accounts*. The total number of cards with an e-money function is the sum of those two subcategories.

Virtual cards are not reported as e-money cards. Only prepaid virtual cards are included. Coupons, gift vouchers that are only accepted by a limited number of sellers are excluded from the reporting of cards on which e-money can be directly stored.

Monetary value stored on specific prepaid instruments does not represent electronic money if the instruments allow the electronic money holder to purchase goods or services only on the premises of the electronic money issuer or within a limited network of service providers under a direct commercial agreement with a professional issuer, or they can only be used to acquire a limited range of goods 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 payment statistics.

Card on which e-money can be stored directly

E-money stored on a card held by an e-money owner. Electronic money means an 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 2007/64/EC, (“payment transaction” means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee) and which is accepted by a natural or legal person other than the electronic money issuer.

This differs them from cards giving access to e-money stored on e-money accounts. These two categories are mutually exclusive.

Card which give access to e-money stored on e-money accounts

Cards which give access to e-money stored on e-money accounts refer to cards that are linked to e-money accounts. It may happen that an e-money card user is not aware of the existence of such an account. A typical example of such a card is a prepaid card. Prepaid cards are often cards that give access to e-money stored on e-money accounts; nevertheless prepaid cards exist that are considered to be cards on which e-money can be stored directly.

E-money account is an account on 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.

Cards with an e-money function which have been loaded at least once

Cards with an e-money function which have been loaded at least one and can thus be considered activated. Loading may be interpreted as indicative of the intention to use the e-money function. All cards that have been loaded are reported under this item,, irrespective of when this loading took place (not necessarily during the reference period). Only cards still valid at the end of the reporting period should be reported.

E-money account

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.

E-money account accessed through a card

In accordance with the definition of “e-money account” and “e-money card”.

E-money payment with cards on which e-money can be stored directly

A transaction whereby the holder of a card with an e-money function transfers e-money value from its balance stored on the card to the balance of the payee/beneficiary.

E-money payment with e-money accounts, of which: accessed through a card

A transaction whereby a card is used to access an e-money account and subsequently funds are transferred from the e-money account of the payer, to the account of the payee.

E-money payments with e-money on accounts

A transaction whereby funds are transferred from the e-money account of a payer, to the account of the payee.

Mobile payment solution

A solution used to initiate payments for which the payments data and the payment instructions are transmitted and/or confirmed via mobile communication and data transmission technology through a mobile device. This category includes digital wallets and other mobile payment solutions used to initiate P2P (person-to-person) and/or C2B (consumer-to-business) transactions, i.e. credit transfers, card payments and/or e-money transactions.

P2P mobile payment solution

A solution where payments are initiated, confirmed and/or received by an individual to another individual (P2P), via a mobile device. The payment instruction and other payment data are

transmitted and/or confirmed with a mobile device. A distinctive mobile payment identifier, such as mobile telephone number or e-mail address, can be used as a proxy to identify the payer and/or payee. P2P mobile payment solutions can be used to initiate credit transfers, card payments and/or e-money transactions.

Strong customer authentication (SCA)

Strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data (Article 4 (30) of Directive (EU) 2015/2366).

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

Authenticated via non-strong customer authentication refers to transactions which are exempted from strong customer authentication pursuant to Chapter III of Commission Delegated Regulation (EU) 2018/389 as well as transactions for which provisions in Article 97(1) of Directive (EU) 2015/2366 do not apply. Merchant initiated transactions as well as other transactions to which SCA is not applicable are included.

Reasons for authentication via non-strong customer authentication (non-SCA)

Low value

Payment transactions for which the exception in Article 16 of the Commission Delegated Regulation (EU) 2018/389 applies:

Payment service providers are not obliged to apply strong customer authentication if payee initiates remote electronic payment transaction and if 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.

Trusted beneficiaries

Payment transactions for which the exception in Article 13 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider,
- the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.

Recurring transaction

Payment transactions for which the exception in Article 14 of the Commission Delegated Regulation (EU) 2018/389 applies:

- the payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee,
- payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions referred above.

Payments to self

Payment transactions for which the exception in Article 15 of the Commission Delegated Regulation (EU) 2018/389 applies: 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. These payments can be credit transfers and e-money transactions.

Secure corporate payment processes and protocols

Payment transactions for which the exception in Article 17 of the Commission Delegated Regulation (EU) 2018/389 applies: Payment service providers shall be allowed not to apply strong customer authentication, 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 for by Directive (EU) 2015/2366.

Transaction risk analysis

Payment transactions for which the exception in Article 18 of the Commission Delegated Regulation (EU) 2018/389 applies, that is:

1. Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.

2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:

- a) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Annex for “remote electronic card-based payments” and “remote electronic credit transfers” respectively;
- b) the amount of the transaction does not exceed the relevant exemption threshold value (‘ETV’) specified in the table set out in the Annex;
- c) payment service providers as a result of performing a real time risk analysis have not identified any of the following:
 - (i) abnormal spending or behavioural pattern of the payer;
 - (ii) unusual information about the payer's device/software access;
 - (iii) malware infection in any session of the authentication procedure;
 - (iv) known fraud scenario in the provision of payment services;
 - (v) abnormal location of the payer;
 - (vi) high-risk location of the payee.

3. Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

- a) the previous spending patterns of the individual payment service user;
- b) the payment transaction history of each of the payment service provider's payment service users;
- c) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;
- d) the identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.

Merchant initiated transaction

Merchant initiated transaction means “Merchant initiated transaction” as defined in Annex II Part C footnote 4 of the EBA Guidelines amending the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) of Directive (EU) 2015/2366 (EBA/GL/2020/01), i.e.: card-based payment transactions that meet conditions specified by the European Commission in Q&A 2018_4131 and Q&A 2018_4031, and which therefore are considered transactions initiated by the

payee and not subject to the obligation to apply strong customer authentication referred to in Article 97 of the Payment Services Directive (PSD2).

Contactless low value

- Contactless payment transactions for which the exception in Article 11 of the Commission Delegated Regulation (EU) 2018/389 applies: the individual amount of the contactless electronic payment transaction does not exceed EUR 50;
- 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;
- 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.

This applies to bank transfers, card-based payment transactions and e-money transactions.

Unattended terminals for transport fares or parking fees

Payment transactions for which the exception in Article 12 of the Commission Delegated Regulation (EU) 2018/389 applies: the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

Fraudulent payments using e-money by fraud origin:

Issuance of a payment order by the fraudster

This is an unauthorised payment transaction, as defined in the Guideline 1.1(a) of the EBA Guidelines on reporting requirements for fraud data under Article 96(6) PSD2: *a) unauthorised payment transactions made, including as a result of 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 (“unauthorised payment transactions”)* and refers to a situation where a fake payment order is issued by the fraudster after having obtained the payer/payee's sensitive payment data through fraudulent means.

Lost or stolen e-money card

A fraud type that occurs with the use of a lost or stolen e-money card without the actual, implied or apparent authority of the card holder.

E-money card not received

An e-money 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 e-money card

The use of an altered or illegally reproduced e-money card, including the replication or alteration of the magnetic strip or embossing.

Unauthorised e-money account transaction

means “unauthorised payment transaction” as defined above in respect to the use of e-money account.

Modification of a payment order by the fraudster

means “modification of a payment order by the fraudster” within the meaning of the Guideline 1.6 (c) of the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) PSD2 (EBA/GL/2018/05), i.e. a type of unauthorised transaction as defined in Guideline 1.1(a) and refers to a situation 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 (for instance through malware or attacks allowing attackers to eavesdrop on the communication between two legitimately communicating hosts (man-in-the middle attacks)) or modifies the payment instruction in the payment service provider’s system before the payment order is cleared and settled.

Losses due to fraud per liability bearer

within the meaning of Guideline 1.6 (b) of the EBA Guidelines on reporting requirements for fraud data under Article 96 (6) PSD2 (EBA/GL/2018/05), i.e.: 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.

2.5. AIS/PIS

Account information service (AIS)

means “account information service” within the meaning of Article 4 (16) of Directive (EU) 2015/2366, i.e.: it means an online service 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 initiation system (PIS)

means “payment initiation system” within the meaning of Article 4 (15) of Directive (EU) 2015/2366, i.e.: it means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.

Account information service provider (AISP)

means “account information service provider” within the meaning of Article 4 (19) of Directive (EU) 2015/2366, i.e.: means a payment service provider pursuing business activities as referred to in point (8) of Annex I (8. Account information service).

Payment initiation service provider (PISP)

means the “payment initiation service provider” within the meaning of Article 4 (18) of Directive (EU) 2015/2366, i.e. “payment initiation service provider” means a payment service provider carrying out business activities as referred to in point (7) of Annex I (7. Payment initiation system).

Payment Service Provider (PSP)

means the “payment service provider” within the meaning of Article 4 (11) of Directive (EU) 2015/2366, i.e.: it means a natural or legal person benefiting from the payment services acting as a payer, payee or both.

Account Servicing Payment Service Provider (ASPSP)

means the “account servicing payment service provider” within the meaning of Article 4 (17) of Directive (EU) 2015/2366, i.e.: it means a payment service provider providing and maintaining a payment account for a payer.

Number of clients

The number of payment service users to which Account Information Service Provider (AISP) offers its services.

Number of payment accounts accessed by Account Information Service Provider (AISP)

The item should provide information on the number of payment accounts with the reporting institution accessed by AISPs based on instruction and consent of the users.

For example: Institution A reports the number of accounts of its clients who gave consent to the provision of institution B, C and D with access to their accounts (within the meaning of Article 2 (4e) of the Act on Payment Services of 19 August 2011 (Journal Laws of No. 2020, item 794, as amended).

Payment account – an account held in the name of one or more users for the purpose of making payment transactions. In this category please specify the total number of payment accounts accessed by an Account Information Service Provider.

Number of clients who gave consent to access their accounts

The reporting agent provides information on the number of its clients (clients who have accounts with that institution) who gave consent to their account with that institution being accessed by the PSP offering account information service.

For example: Institution A reports the number of clients who have given consent to their account with institution A being accessed by institution B.

Number of clients of Account Information Service Providers

Information should be provided on the number of users who have transmitted to PSP offering account information service consent to access their account.

For example: Institution A reports the number of clients who have given consent to institution A to access their account with institution B.

Number of payment accounts held by clients of account information service providers

Number of accounts to which access was given to the account information service provider.

Number of clients of payment initiation service providers

The payment initiation service consists in the initiation by an entity authorised to provide such a service, at the request and on behalf of the user, of a payment order (credit transfer) from the user's payment account.

2.5.1. Detailed information on the reported tables

Information reported by credit institutions, payment institutions and account information service providers:

1. Account Servicing Payment Service Provider (ASPSP) perspective

1.1.1/2.1.1 Number of payment accounts accessed by Account Information service providers (AISP) broken down by the country of residence of the AISP with account access.

Each account is reported only once, only in one of the countries, in accordance with the following principles:

- the country reported is the country from which access is made most frequently,
- if the account has been accessed from a number of countries and the access frequency in terms of the number of inquiries per a given account was the same, the country reported is the country from which access was made most recently in a given reporting period,
- the accounts reported are only those to which access in the reporting period is made at least once
- domestic ASPSP report the number of accounts accessed by a Polish AISP in the column marked as "U6", whereas ASPSP operating across borders report the number of accounts accessed by a Polish AISP in the column marked as "PL",
- domestic ASPSP report the number of accounts accessed by a AISP operating across borders (e.g. the Austrian entity) in the column designated with a code of the country of its location (e.g. AT),

1.1.2/2.1.2 Number of clients who gave consent to access their account (without geographical breakdown). The number of clients reported is the number of clients who own the accounts reported in item 1.1, and were customers of the ASPSP on the last day of the reporting period, according to the following principles:

- each client is reported only once, regardless of the number of accounts made available in a given reporting period.
- reported are all those clients who viewed their account (or one of their accounts) from their AISP account during the reporting period (i.e. their account was accessed at least once).

1.2.2/2.2.2 – Number of clients of Account Information Service Providers, broken down geographically by country of citizenship (residence) of the customer according to the rules:

- All clients who have ever given consent to the service and continue to do so and were still clients on the last day of the reporting period are reported, irrespective of whether these clients have used the service or not,
- domestic AISP report the number of clients who are Polish citizens in the column marked as "U6", and AISP operating across border report the number of clients who are Polish citizens in the column marked as "PL",
- domestic AISP report the number of clients who are foreign citizens (e.g.: Austrian) in the column designated with the code of the country of their citizenship (e.g.: AT).

2. Account Information Service Provider (AISP) perspective

1.2.1/2.2.1 Number of payment accounts held by clients of account information service providers (without geographical breakdown), i.e. the number of accounts that the reporting AISP has access to on the basis of client consents as indicated in section 1.2.2/2.2.2/3.2.2

The total number of accounts for which consent has ever been granted, and was valid as at the last day of the reporting period (i.e. your client is still using the service and has not withdrawn consent) is reported for this item.

Number of clients of account information service providers broken down geographically by country of citizenship (residence) of the client according to the rules:

- all clients who have ever granted consent to the service and continue to do so and were still clients on the last day of the reporting period are reported, irrespective of whether these customers have used the service or not,
- domestic AISP report the number of clients who are Polish citizens in the column marked as “U6”, and AISP operating across border report the number of clients who are Polish citizens in the column marked as “PL”,
- domestic AISP report the number of clients who are foreign citizens (e.g.: Austrian) in the column designated with the code of the country of their citizenship (e.g.: AT).

3. *PISP perspective*

1.3/2.3 Number of clients of payment initiation service providers (without geographical breakdown).

The total number of clients who used the PIS service at least once during the reporting period and were clients on the last day of the reporting period is reported.

Each client is reported only once, regardless of the number of services initiated in a given reporting period.

Initiated by PISP

An item reported by an account servicing payment service provider (ASPSP), Reporting agents, ASPSP, should include payments initiated by external PISPs on behalf of payers that have payment accounts with that particular reporting PSP.

PIS table

In the “PL” column, only PISPs operating in Poland in the framework of cross-border activities are reported. They will report in this column the payment initiation services for which the transaction was sent from an account of a Polish resident entity (i.e. from an account belonging to an ASPSP based in Poland).

In turn, column marked as “W2” is filled in by resident PISPs (i.e. PISPs located in Poland) providing payment initiation services based on which a transaction was sent from an ASPSP account based in Poland.

If, under a payment initiation service, a transaction was executed from an ASPSP account based in Germany, then such a service will be reported in the DE column.

Payment initiation services should be reported for which payment has been executed, i.e. funds have been transferred. PIS transactions with the status transmitted, scheduled or pending are not reported until they change status to executed, i.e. where the payment, as a result of a service order, has been finalised.

Cancelled or rejected transactions should not be included in the statistics.

Number and value of payment initiation services PIS.01 The number and value of payment initiation services are reported in the AIS/PIS taxonomy by providers of payment initiation services (PISPs). These tables report on PIS services (transaction initiation only) for which the reporting agent is the provider, i.e. where a customer initiates a payment order via a PISP in relation to a payment account held with another PSP (as a result of the initiation of a payment service, the next step of the transaction occurs, which is the execution of the payment by the client's ASPSP, which is not reported in this table). The geographical breakdown relates to the residence (country of domicile) of the ASPSP that operates the account from which the payment is made (by the ASPSP).

Example 1 (PISP – PL, Payee’s account – PL, Payer’s account – any country)

A PISP located in Poland (reporting agent) that initiates a transaction from an account of an ASPSP located in Poland reports a given transaction of the PIS in column “W2” (domestic). This will be the most common category of reported transactions.

The account of the recipient of the transaction does not matter in this case, it can be serviced by an ASPSP based either in Poland or abroad.

Example 2 (PISP – PL, Payee’s account – PL, Payer’s account – any country)

A PISP based in Poland (reporting agent) that initiates a transaction from an account of ASPSP based in Austria reports the PIS service in question in column “AT” (Austria).

The account of the recipient of the transaction does not matter in this case, it can be handled by an ASPSP based either in Poland or abroad.

Example 3 (PISP – no PL, Payee’s account – PL, Payer’s account – any country)

A PISP located outside Poland (reporting agent) that initiates a transaction from an account of ASPSP located in Poland reports the PIS service in question in column “PL” (Poland).

The account of the recipient of the transaction does not matter in this case, it can be held with an ASPSP based either in Poland or abroad.

These payment initiation services are reported by PISP. In contrast, transactions resulting from the initiation of a PIS service are also reported by ASPSP as a separate item in the WIP2 taxonomy – such transactions are reported by Payment Instrument Issuers in Tables 4a.L and 4a.W (item 4.4.1) (or in fraud tables 5a.LF, 5a.WF).

The PISP reports only those payment initiation services for which the PISP has provided the ASPSP with all necessary and correct information to enable the ASPSP to complete the payment transaction. The outcome of service delivery can be:

- the execution of a transfer order or other payment transaction by the ASPSP (a funds transfer has taken place),
- or the rejection by the ASPSP of a correctly submitted credit transfer order due to e.g.: lack of funds on the customer's account or exceeding the limits defined on the account.

'Scheduled' or 'pending' payment initiation service transactions are not reported by PISP. When the aforementioned transactions change status to 'completed', i.e. when the necessary and correct information has been successfully transmitted to the ASPSP for the ASPSP to complete the payment transaction, then the PISP should report such transaction to NBP.

Number and value of fraudulent payment initiation service transactions. All PIS transactions and fraudulent transactions are reported in Table PIS.01. In Table PIS.02 only fraudulent PIS transactions are reported (transactions reported in Table PIS.02 are a subset of the transactions from Table PIS.01).

Transactions are reported in PLN.

3. Access to Payment Statistics Database – BSP system

3.1. Access to Payment Statistics Database – BSP

The Payment Statistics Database (BSP system) is integrated with the ZSZT (Integrated Identity Management System) and the Reporting Information System Web Portal (SIS Portal).

The transmission of reports to the BSP system, in the form of XBRL instance files, shall be made electronically via the SIS Portal, accessible at the following address <http://sis.nbp.pl>

Detailed information on the functionality and available user roles in the system is contained in the document 'SIS Portal User Guide', which can be downloaded from the SIS Portal.

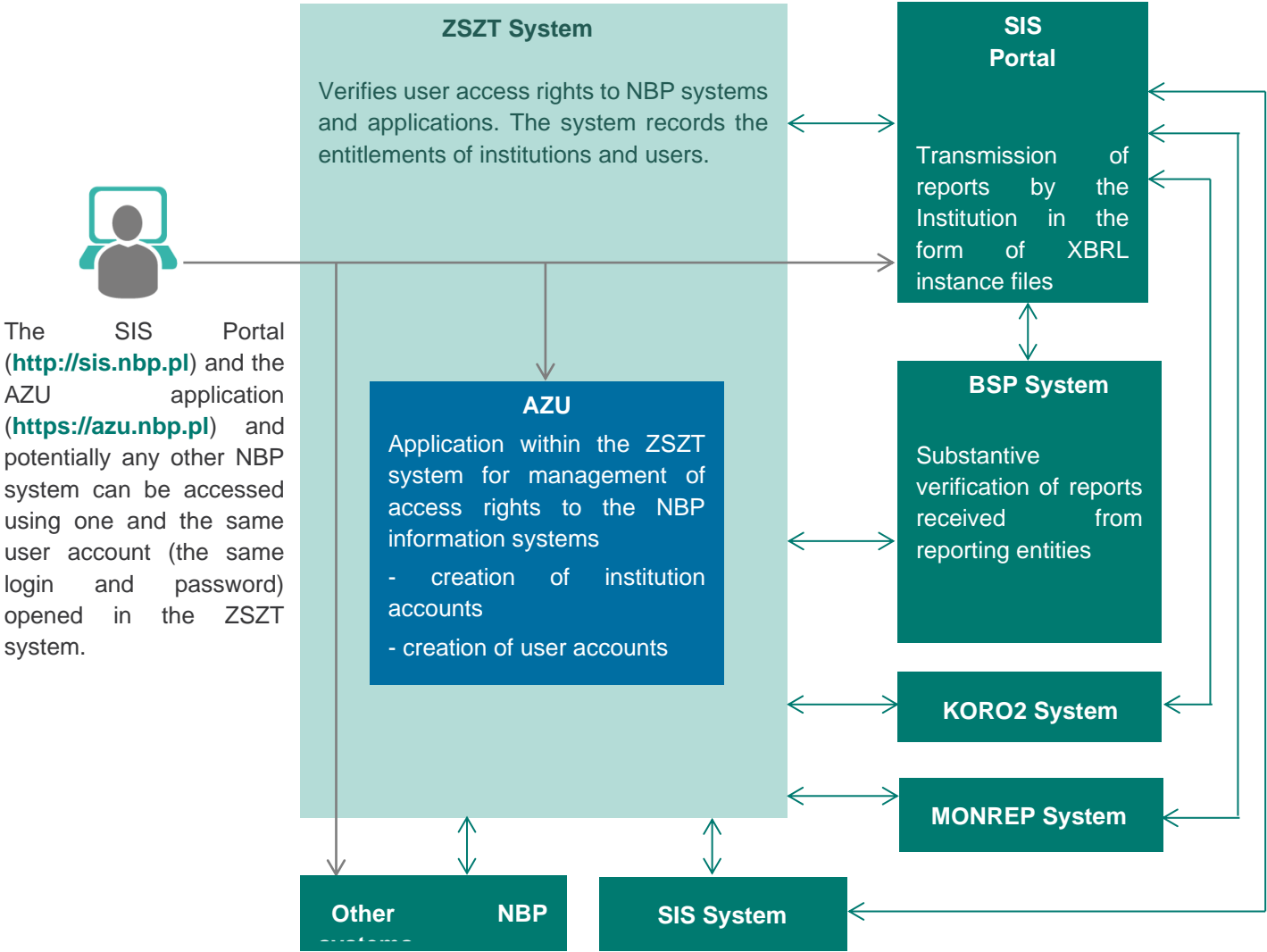
Zintegrowany System Zarządzania Tożsamością (ZSZT) is a system that is used to manage access to NBP systems, such as: BSP, KORO2, MONREP, SIS (and indirectly Portal SIS).

This system includes:

- institution accounts – authorisation to a particular NBP system, e.g. the BSP system. The institution's account is certified to use information systems.
- the institution's user accounts – the permissions for a given user within the system. The following types of users are distinguished in the ZSZT system:
 - An Authorisation Administrator for the Institution (AUI) (account with login and password) – issues requests for opening accounts for new users of the institution, changes their access rights, passwords or user data, sends reports via the SIS Portal.
 - An account without administrative rights with authorisations (account with login and password) assigned by AUI. The user can send reports via the SIS Portal (if the AUI assigns to it such authorisations).

As part of the ZSZT, **Aplikacja Zarządzania Użytkownikami (AZU)** has been set up to manage access to the NBP systems, i.e. to manage institution accounts and institution user accounts. The AZU application is available at <https://azu.nbp.pl>

The links between the BSP system and the ZSZT system and the SIS Portal systems are shown in the diagram below.




The document that describes the functioning of ZSZT (including AZU) is *Regulations on Authentication of External Users in Information Systems of the National Bank of Poland within the Integrated Identity Management System* (Resolution No. 65/2016 of the NBP Management Board of 24 November 2016). Requests (appendices to the aforementioned *Regulations*) for opening account in the ZSZT system (and thus for the BSP system) and manuals for the AZU users are available on the following website <http://www.nbp.pl/azu> (<http://www.nbp.pl/azu/dokumenty.aspx>).

AZU







- [Strona główna](#)
- [Czym jest AZU?](#)
- [Poznaj AZU \(instrukcje\)](#)
- [Lista dokumentów](#)

Aplikacja Zarządzania Uprawnieniami — AZU

Lista dokumentów

 [Uchwała Nr 20/2018 Zarządu Narodowego Banku Polskiego z dnia 25 maja 2018 r. w sprawie wprowadzenia „Regulaminu uwierzytelniania użytkowników spoza Narodowego Banku Polskiego w systemach informatycznych w ramach Zintegrowanego Systemu Zarządzania Tożsamością”](#)

Załączniki do Regulaminu – Wnioski

-  [Wniosek o założenie konta/nadanie uprawnień/delegowanie roli do zarządzania uprawnieniami dla instytucji](#)
-  [Wniosek o założenie/aktywowanie/przedłużenie ważności /nadanie uprawnień dla konta użytkownika](#)
-  [Wniosek o wyznaczenie Administratora Uprawnień Instytucji](#)
-  [Wniosek o wycofanie uprawnień dla Administratora Uprawnień Instytucji](#)
-  [Wniosek o wycofanie uprawnień dla konta użytkownika w systemie informatycznym](#)
-  [Wniosek o wycofanie uprawnienia/ delegowania roli do zarządzania uprawnieniami instytucji w systemie informatycznym](#)

In order to obtain access to the BSP system:

- submit a request for opening an institution account in the BSP information system (Appendix 1 to the aforementioned Regulations).

The request form includes the following item: *Institution Certificate YES, NO*. The certificate is obligatory. The certificate guarantees safe connection with the NBP systems.

When institutions submit reports to several systems (BSP, MONREP, SIS, KORO2), a request whose template constitutes Appendix 1 is submitted for each such system, and the item *Institution Certificate* can be marked as “YES” only in the first request submitted, because one certificate applies to all systems set forth in the ZSZT system.

The rules for issuing and collecting certificates for the purposes of authentication and authorisation in the NBP information systems are specified in “DOCert System – Certification Policy for User Certificates” available on the website: www.docert.nbp.pl

Certificates are collected in person at the regional branches of NBP. The waiting time for a certificate to be issued at the regional branch in Warsaw is approximately three weeks.

Institutions that intend to collect the certificate in Warsaw may apply an alternative and faster procedure for receiving the certificate. Institution may request to be granted a one-off code by the NBP Headquarters, and then go to www.docert.nbp.pl in order to enter the remote certificate system SZOC and generate a certificate using the one-off code granted. Institutions that are interested in using the aforementioned path should enter “NBP Headquarters” in the certificate collection place field.

In the item 1. *Institution data*: of the request please specify the type of the report(s) sent (e.g.: AR1, WIP1), in accordance with the table below:

| Type of report | Reports sent by: |
|----------------|---|
| AR1 | Acquirers (ST forms) |
| AR2 | Acquirers 2 |
| WIP1 | Payment instrument issuers (FN forms) |
| WIP2 | Payment instrument issuers 2 |
| WW | Cash deposit and withdrawal at bank's cash desks |
| WPE2 | Electronic money issuer 2 |
| WIPE2 | Electronic money instrument issuer 2 |
| Poczta | State enterprise of public utility – Poczta Polska |
| AIS_PIS | AIS/PIS services |
| SP | Payment system |
| KIR-K | Clearing houses (KIR form on a quarterly basis) |
| PP | Economic operators pursuing business activity in the field of execution and intermediation in execution of money remittances in domestic and foreign transactions |

2. Please submit a request for opening an account for the Authorisation Administrator of the Institution in Zintegrowany System Zarządzania Tożsamością (ZSZT), the template of which constitutes Appendix 2 to the aforementioned *Regulations*.

Having completed the registration process, the person listed as first in the request submitted is granted a login and password that enables her/him to access the AZU Application and the SIS Portal. In the AZU Application, the first of the Authorisation Administrators of the Institution (AUI) is able to issue requests for opening accounts for new users and to assign to them appropriate authorisations.

NOTE: The requests submitted must be marked with a company stamp of the institution and with personal stamps and signatures of the persons authorised to make declarations of will on behalf of the institution.

Written requests shall be sent to:

Departament Systemu Płatniczego
Narodowy Bank Polski
ul. Świętokrzyska 11/21
00-919 Warszawa
with the following annotation "BSP System Request"

Reports can be sent to the BSP system via SIS Portal.

Access to the BSP system is granted to institutions which are obliged to submit reports under the following regulations:

1. Regulation of the Minister of Finance of 22 December 2022 *on providing information to Narodowy Bank Polski by acquirers, payment instruments issuers and electronic money issuers* (Journal of Laws, item 2819),
2. Regulation of the Minister of Finance of 19 December 2022 *on providing data to Narodowy Bank Polski for the assessment of the functioning of monetary and interbank settlements* (Journal of Laws, item 2766).

3.2. Access to the test environment of the BSP system

The BSP system's test environment is analogous to the BSP system's production environment. The test BSP system is integrated with the test systems of the SIS Portal and ZSZT.

In order to be granted access to the test BSP system please contact NBP by e-mail (to system.platniczy-dane@nbp.pl), with "Access to the test environment of the BSP system" in the subject line.

The test system of the SIS Portal is available on <https://sisrozw2u.nbp.pl/> and the test environment of the AZU application can be accessed at <https://azu-test.nbp.pl>

3.3. Useful links

- AZU User Manuals (Certificate Installation Manual, AZU Manual for External Users)
<http://www.nbp.pl/azu>
<http://www.nbp.pl/azu/dokumenty.aspx>
- Rules for Issuing and Collecting Certificates www.docert.nbp.pl
- Test environment of the SIS Portal <https://sisrozw2u.nbp.pl/>
- Test environment of AZU <https://azu-test.nbp.pl>
- Production environment of the SIS Portal <http://sis.nbp.pl>
- Production environment of AZU <https://azu.nbp.pl>

4. Access to SIS Portal and to AZU

4.1. First access to SIS Portal and AZU for the BSP system

Before logging on for the first time to SIS Portal or to AZU, each user must install a certificate on their workstation in accordance with the manual provided on the website <http://www.nbp.pl/azu/poznaj.aspx>



AZU

Strona główna

Czym jest AZU?

Poznaj AZU (instrukcje)

Lista dokumentów

Aplikacja Zarządzania Uprawnieniami — AZU

Poznaj AZU

-  Instrukcja obsługi Aplikacji Zarządzania Uprawnieniami (AZU) dla Administratorów Upnień Instytucji (AUI) w Zintegrowanym Systemie Zarządzania Tożsamością (ZSZT)
-  Instrukcja obsługi Aplikacji Zarządzania Uprawnieniami (AZU) dla użytkowników zewnętrznych (UZ) w Zintegrowanym Systemie Zarządzania Tożsamością (ZSZT)
-  Wykaz skrótów i definicji
-  Instalacja certyfikatu
Warunkiem poprawnej autoryzacji użytkownika w aplikacji AZU jest zainstalowanie tzw. klucza firmowego w przeglądarce internetowej, wydanego przez NBP w systemie DOCert NBP.

Having installed the certificate and received a login and password to AZU system and to SIS Portal (one account with the same password), the user should log in to AZU in order to change the password and accept the regulations in force at Narodowy Bank Polski in the documents made available at the link provided.

After they have accepted the aforementioned regulations, users are granted access to the SIS Portal. Failure to accept the regulations shall result in users being unable to use the NBP systems, and in particular the SIS Portal.

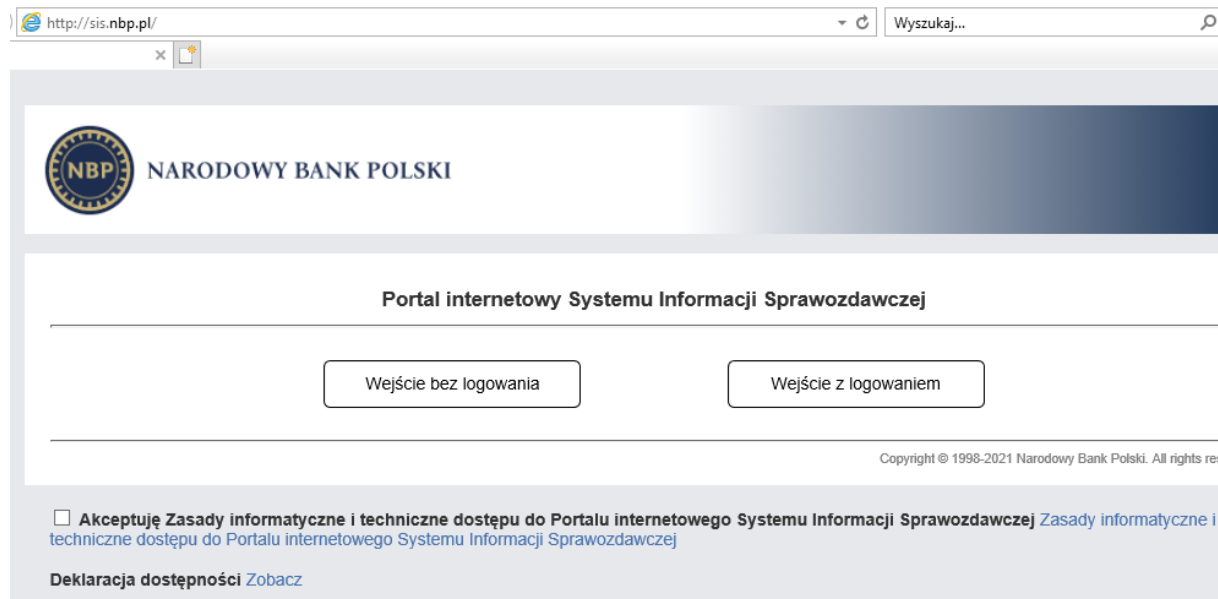
Note!

If a user is unable to transmit reports via the SIS Portal (has no access to the SIS portal), this may be caused by the following events:

- the user failed to accept the aforementioned regulations,
- the AUI of your institution failed to grant the user the relevant authorisations to submit reports (for details see *AZU System – Working Environment*)
- the user tried to log in to the SIS Portal too soon, i.e. within 15 minutes after the acceptance of the aforementioned regulations in AZU.

4.2. SIS Portal – Working Environment

The working environment of the SIS Portal is available at <http://sis.nbp.pl>



The functionality of the SIS Portal allows for:

1. mandatory XBRL taxonomies to be downloaded for individual reporting periods,
2. reports in the XBRL format to be submitted in accordance with the taxonomy published by NBP,
3. reports in the XBRL format to be verified in terms of their correct structure, semantics (compliance with the taxonomy of reporting information) and contents (compliance with audit principles),
4. information to be exchanged with reporting agents in the Information Centre.

The SIS Portal can be accessed by guest users, i.e. users that do not have user accounts and have not been granted a login and password. Guest users may access the SIS Portal at workstations on which a certificate granted by the institution has been installed. Guest users have access exclusively to the information centre, taxonomies and can send test reports. Test reports that are sent by guest users are not delivered to the BSP system. This functionality is made available to reporting agents only for the purposes of verifying of whether the report compiled is correct, i.e. for the purposes of testing whether it can be successfully submitted in the working environment.



Testowe przesłanie sprawozdań

System:

Okres sprawozdawczy:

Rodzaj sprawozdania:

4.2.1. SIS Portal User Manual

The functionalities of the SIS Portal have been detailed in the *SIS Portal User Manual* which can be downloaded from the *Information Centre* of the SIS Portal. In order to download the aforementioned document please:

1. Log into the SIS Portal
2. Expand the *Information Centre [Serwis Informacyjny]* menu and select the *Documents [Lista dokumentów]*

Strona główna Serwis informacyjny ▾ Sprawozdawczość ▾ Administracja ▾ Taksonomie Wylogowanie

Serwis informacyjny ▾
Lista dokumentów
Lista publikacji

| Tytuł publikacji | Data publikacji |
|--|-----------------|
| Dokument test | 2019-07-18 |
| Instrukcja użytkownika Portalu internetowego Systemu Informacji Sprawozdawczej | 2017-04-12 |

3. Select **SIS Portal User Manual [Instrukcja użytkownika Portalu internetowego Systemu Informacji Sprawozdawczej]**

4.2.2. Submission of reports via SIS Portal to the BSP system (working environment)

In order to submit reports in the XBRL format in the working environment of the SIS Portal, the user must:

1. Expand the *Reporting [Sprawozdawczość]* menu and select *Submit reports [Przesyłanie sprawozdania]*



Produkcyjne przesłanie sprawozdań

System:

Okres sprawozdawczy:

Rodzaj sprawozdania:

2. Select *BSP System* [System BSP] and relevant *Reporting period* [Okres sprawozdawczy] and *Report type* [Rodzaj sprawozdania] e.g.:



Produkcyjne przesłanie sprawozdań

System:

Okres sprawozdawczy:

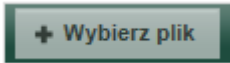
Rodzaj sprawozdania:

- Wybierz
- AIS/PIS Usługi
- AR1 - Agent rozliczeniowy 1
- AR2 - Agent rozliczeniowy 2
- Biura Usług Płatniczych
- Działalność depozytowa
- Działalność rozliczeniowa
- Działalność rozrachunkowa
- KIR kwartalne

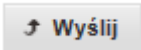
The user may select the following reports:

| Item | Report type | Taxonomy symbol | Abbreviated name |
|------|--|-----------------|------------------|
| 1 | Acquirer 1 | AR1 | AR1 |
| 2 | Acquirer 2 | AR2 | AR2 |
| 3 | Payment instrument issuer 1 | WIP1 | WIP1 |
| 4 | Payment instrument issuer 2 | WIP2 | WIP2 |
| 5 | Cash deposit and withdrawal at bank's cash desks | WW | WW |
| 6 | Electronic money issuer 2 | WPE2 | WPE2 |
| 7 | Electronic money instrument issuer 2 | WIPE2 | WIPE2 |
| 8 | AIS/PIS services | AIS/PIS | AIS/PIS |
| 9 | Payment system | SP | SP |
| 10 | Poczta Polska | POCZTA_POLSKA | Post |
| 11 | KIR quarterly | IR_KIR_K | KIR-K |
| 12 | National/international money transfers | PRZEK_PIEN | PP |

3. Attach the file of the report in the XBRL format by pressing

A rectangular button with a dark green background and white text that reads "+ Wybierz plik".

4. Submit the report by pressing


A rectangular button with a light grey background and dark grey text that reads "Wyślij" with a small upward-pointing arrow icon to its left.

4.3. AZU – working environment

AZU is a website application (portal) that enables institutions through their authorised employees (Authorisation Administrators of the Institution) to manage authorisations granted to their employees to access the NBP systems integrated in ZSZT (in particular the SIS Portal). The application makes key information available to its registered users.

The working environment of AZU is available at <https://azu.nbp.pl>

← → ↻ 🏠 azu.nbp.pl/my.policy ☆ ⚙️ 🗄️ 👤 ⋮



NARODOWY BANK POLSKI

Aplikacja Zarządzania Uprawnieniami

Aplikacja Zarządzania Uprawnieniami

Nazwa użytkownika

Hasło

Zaloguj

Copyright by Narodowy Bank Polski. All rights reserved.

Any necessary user manuals for ZSZT and AZU are available at <http://www.nbp.pl/azu/poznaj.aspx>, and in particular, the following ones:

- AZU User Manual for Authorisation Administrators of the Institution (AUI) in ZSZT
- AZU User Manual for External Users in ZSZT
- List of abbreviations and definitions
- Certificate installation



NARODOWY BANK POLSKI

AZU

- Strona główna
- Czym jest AZU?
- Poznaj AZU (instrukcje)**
- Lista dokumentów

Aplikacja Zarządzania Uprawnieniami — AZU

Poznaj AZU

-  Instrukcja obsługi Aplikacji Zarządzania Uprawnieniami (AZU) dla Administratorów Upnień Instytucji (AUI) w Zintegrowanym Systemie Zarządzania Tożsamością (ZSZT)
-  Instrukcja obsługi Aplikacji Zarządzania Uprawnieniami (AZU) dla użytkowników zewnętrznych (UZ) w Zintegrowanym Systemie Zarządzania Tożsamością (ZSZT)
-  Wykaz skrótów i definicji
-  Instalacja certyfikatu
Warunkiem poprawnej autoryzacji użytkownika w aplikacji AZU jest zainstalowanie tzw. klucza firmowego w przeglądarce internetowej, wydanego przez NBP w systemie DO Cert NBP.

In AZU, Authorisation Administrators of the Institution are entitled to:

1. grant themselves and other (existing) users of the institution the relevant authorisations to submit reports to the BSP system,
2. submit requests for opening accounts in the BSP system for new users.

1. Granting of authorisations to submit reports by the Authorisation Administrators of the Institution

- Please select the *INSTITUTIONS [INSTYTUCJE]* menu in AZU
- Select the Institution (the example shown concerns the granting of authorisation to NBP)

Zarządzasz instytucją: Narodowy Bank Polski

Nazwa: Narodowy Bank Polski

- Select *SIS BSP BSP reporting agent [Sprawozdawca BSP]* as shown in the screenshot below:

Delegowane uprawnienia Instytucji w aplikacji

▼ Filtr: Wyczyść

| Nazwa aplikacji | Nazwa roli | Opis |
|-----------------|--|--|
| | Administrator Uprawnień Instytucji (AUI) | Zarządca wszystkimi uprawnieniami tej instytucji |
| EWIB2 | Rola dla czytelników zewnętrznych | Czytelnicy zewnętrzni |
| EWIB2 | Rola dla edytorów zewnętrznych | Edytorzy zewnętrzni |
| SIS BSP | Odbiorca publikacji dedykowanej BSP | Rola dla użytkownika, umożliwia dostęp do publikacji dedykowanej |
| SIS BSP | Sprawozdawca BSP | Rola dla użytkownika, umożliwia wysyłanie sprawozdań, obowiązowa dla Instytucji sprawozdającej |

- Enter *Name, Surname and PESEL number [Imię, Nazwisko i ID PESEL]* of the user to be granted authorisations to submit reports to the BSP System
- Having entered the relevant user data please select *Add user as requested [Dodaj użytkownika według kryterium]*

2. Opening accounts for new users

- Please select the *REQUESTS [WNIOSKI]* menu in AZU
- Select *User accounts [Konta użytkowników]*

Aktywne wnioski czekające na Ciebie: 0

Wystaw nowy wniosek dotyczący:

- [Dostępu do aplikacji](#)
- [Kont użytkowników i stacji roboczych](#)

Sprawdź status wniosku

- [Wyszukaj wniosek](#)

- Select “Request for opening account for an external user by the Authorisations Administrator of the Institution” [Utworzenie konta użytkownika zewnętrznego przez Administratora Uprawnień Instytucji]

Wynik wyszukiwania. Wybierz nowy wniosek, który chcesz wystawić

| Rodzaj wniosku | Opis |
|--|--|
| Aktywacja lub wydlużenie konta użytkownika zewnętrznego | Wniosek o aktywację lub wydłużenie konta użytkownika zewnętrznego |
| Dezaktywacja konta użytkownika zewnętrznego | Wniosek o dezaktywację konta użytkownika zewnętrznego |
| Nadanie uprawnień Administratora Uprawnień Instytucji dla konta użytkownika zewnętrznego | Wniosek o nadanie dla konta użytkownika zewnętrznego uprawnień Administratora Uprawnień Instytucji |
| Odebranie uprawnień Administratora Uprawnień Instytucji | Wniosek o odebranie uprawnień Administratora Uprawnień Instytucji |
| Utworzenie konta użytkownika zewnętrznego | Wniosek o utworzenie konta użytkownika zewnętrznego |
| Utworzenie konta użytkownika zewnętrznego w roli Administratora Uprawnień Instytucji | Wniosek o utworzenie konta użytkownika zewnętrznego w roli Administratora Uprawnień Instytucji |

Donnie

Strona 1/1

Następne

Other functionalities have been described in detail in the aforementioned manuals.

5. Requirements for preparation of XBRL files

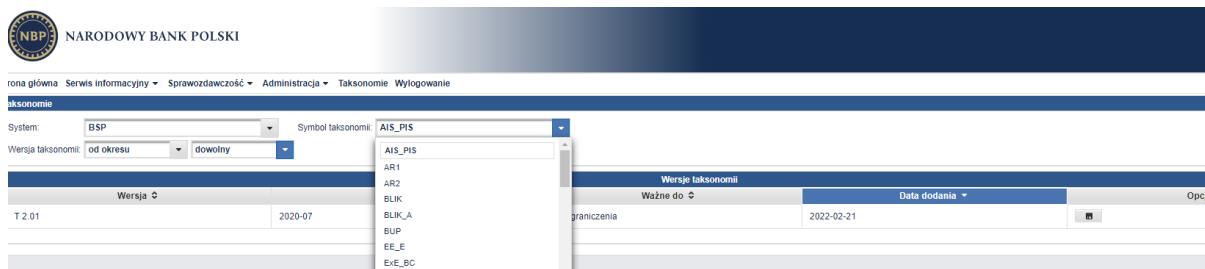
5.1. Data submission format


Reports on the payment service market must be submitted to NBP by reporting agents in the form of XBRL files in accordance with the XBRL taxonomies developed by NBP. Taxonomies and validation formulas are available for downloading at the SIS Portal at the following websites: <http://sis.nbp.pl> and <https://sis.nbp.pl>

Reports in the form XBRL instance files are submitted to NBP via the SIS Portal available at <https://sis.nbp.pl>. Reports are subject to validation. When successfully validated, reports are delivered to the BSP System.

In order to download taxonomies from the SIS Portal please:

1. Log into the SIS Portal
2. Select *Taxonomies [Taksonomie]*
3. Select *System: BSP* and next select a relevant *Taxonomy symbol [Symbol taksonomii]* from a drop-down list e.g.: *AIS_PIS*



4. Please select the relevant file and press  in the table with taxonomies (column: *Options [Opcje]*)

Note:

It is recommended that reports are submitted in the *.zip format. Files in the original format (*.xml) are acceptable however only if they do not exceed 10 MB.

www.nbp.pl