Instruction No. 2

On reporting requirements on statistical information on frauds related to means of payment

THE FINANCIAL INFORMATION AUTHORITY

having regard to Article 62 (3) of Regulation No. 3 *on payment services provided by entities carrying out financial activities on a professional basis* of 23 May 2018, according to which entities carrying out financial activities on a professional basis, that are payment service providers in accordance with Article 4 (27) of the same Regulation No. 3, shall provide, at least on an annual basis, statistical data on fraud relating to different means of payment to the Financial Information Authority;

whereas the identification of the statistical information on frauds related to payment transactions initiated and executed, including payments by payment cards, is necessary to allow payment service providers to comply with the obligations established by the regulatory framework on services of payment in place;

taking into account the guidelines adopted by relevant international and European bodies on the matter;

giving execution of the resolution adopted by the Board of Directors on 5 April 2018;

PROMULGATES THE FOLLOWING INSTRUCTION

Title I

Scope of application, object and definitions

Article 1. *Scope of application.*

This Instruction applies to entities carrying out financial activities on a professional basis within the State, authorized for issuing and managing of means of payment and within the scope of application of Regulation No. 3 of 23 May 2018.

Article 2. *Object.*

1. This Instruction is about the reporting on statistical information indicated in Article 62 (3) of Regulation No. 3 of 23 May 2018.

2. Payment service providers shall report to the Financial Information Authority:

a) statistical information on frauds related to to different means of payment that have been initiated and executed, including frauds that have been initiated by a payment initiation service provider;

b) statistical information on attempted and not executed activities, operations or transactions related to different means of payment, reported under Article 40 (1) of Law no. XVIII of 8 October 2013.

3. The statistical information reports referred to in paragraph 2 (a) shall be carried out according to Title II.

In any case, payment service providers shall not include statistical information on payment transactions that, however linked to any of the circumstances referred to in paragraph 2 (a), have not been executed and have not resulted in a transfer of funds.

4. The statistical information reports referred to in paragraph 2 (b) shall be carried out according to a scheme independently defined by payment service providers.

Article 3. *Definitions.*

1. To the ends of this Instruction, the same definitions under Article 4 of Regulation No. 3 of 23 May 2018 apply, as well as the following definitions.

2. «*Issuance of a payment order by the fraudster*»: a type of unauthorized transaction that 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.

3. «*Domestic payment transaction*»:

a) for non-card based payment transactions, and remote card based payment transactions: payment transaction initiated by a payer, or by or through a payee, where the payer's payment service provider and the payee's payment service provider are located in the same jurisdiction;

b) for non-remote card-based payment transactions: payment transaction where the payer's payment service provider (issuer), the payee's payment service provider (acquirer) and the point of sale (POS) or automated teller machine (ATM) used are located in the same jurisdiction;

c) for payment initiation services: payment transaction where the payment initiation service provider and the account servicing payment service provider are located in the same jurisdiction.

4. «*Total fraudulent payment transactions*»: sum of «*unauthorized payment transactions*» and «*manipulations of the payer*».

5. «*Unauthorized payment transactions*»: 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.

6. «*Cross-border payment transactions outside the European Economic Area*»:

a) for payment transactions: payment transaction initiated by a payer, or by or through a payee, where either the payer's or the payee's payment service provider is located outside the European Economic Area while the other is located within the European Economic Area.

b) for payment initiation services: payment transaction, where the payment initiation service provider is within the European Economic Area and the account servicing payment service provider is located outside the European Economic Area.

7. «*Cross-border payment transactions within the European Economic Area*»:

a) for non-card based payment transactions and remote card based payment transactions: payment transaction initiated by a payer, or by or through a payee, where the payer's payment service provider and the payee's payment service provider are located in different jurisdictions within the European Economic Area;

b) for non-remote card-based payment transactions: payment transactions where the payer's payment service provider (issuer) and the payee's payment service provider (acquirer) are in different member states or the payer's payment service provider (issuer) is located in a different jurisdiction within the European Economic Area jurisdiction from that of the point of sale (POS) or automated teller machine (ATM);

c) for payment initiation services: payment transaction where the payment initiation service provider and the account servicing payment service provider are located in different jurisdictions within the European Economic Area.

8. «*Manipulations 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.

9. «*Modification of a payment order by the fraudster*»: a type of unauthorized transaction that 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.

10. «*Losses due to fraud per liability bearer*»: losses by the reporting payment service provider, its payment service user or others, reflecting the actual impact of fraud on a cash flow basis.

11. «*Payment service providers*»: entities carrying out financial activities on a professional basis within the State, authorized for issuing and managing of means of payment and within the scope of application of Regulation No. 3 of 23 May 2018, that fall within the scope of application of this Instruction

12: «*European Economic Area*»: geographical area that includes Member States of the European Union, European Free Trade Association participating jurisdictions (excluding Switzerland) and, to the ends of this Instruction only, Single Euro Payments Area participation jurisdictions.

Title II

Statistical information reports on frauds related to different means of payment

Article 4. *General requirements.*

1. Payment service provider shall report statistical information on:

a) total payment transactions, in line with the different breakdowns provided in the Annex and in accordance with Article 5; and

b) total fraudulent payment transactions in line with the different breakdowns provided in the Annex and in accordance with Article 7.

2. Payment service providers shall report the statistical information referred to in paragraph 1 in terms of both volume (i.e. number of transactions or fraudulent transactions) and value (i.e. amount of transactions or fraudulent transactions).

Volumes and values shall be reported in actual units, with two decimals for values.

3. The values shall be reported in euro currency.

For payment transactions denominated in a currency other than the euro currency, payment service providers shall convert data for values into euro currency, using the relevant exchange rates applied to these transactions or the average European Central Bank reference exchange rate for the applicable reporting period.

The methodology used shall be reported.

4. Payment service providers shall identify the applicable data breakdown(s) indicated into the Annex, depending on the payment service(s) and payment instrument(s) provided, and submit the applicable statistical information.

The *ratio* behind decisions on applicability shall be reported.

5. Payment service providers shall allocate each transaction to only one sub-category for each row of each data breakdown.

6. In the case of a series of payment transactions being executed, or fraudulent payment transactions being executed, payment service providers shall consider each payment transaction or fraudulent payment transaction in the series to count as one.

7. Payment service providers shall ensure that all statistical information reported to the Financial Information Authority can be cross-referenced in accordance with the Annex.

Article 5. *Fraudulent payment transactions.*

1. Payment service providers shall report statistical information on the following typologies of fraudulent payment transactions, for each reporting period:

a) unauthorized payment transactions;

b) manipulations of the payer.

2. Payment service providers shall report the statistical information related to all payment transactions and fraudulent payment transactions, in accordance with the following:

a) total fraudulent payment transactions shall be reported regardless of whether the amount of the fraudulent payment transaction has been recovered;

b) losses due to fraud per liability bearer, as well as the final fraud losses, shall be reported in the period when they are recorded in the payment service provider's books, without taking into account refunds by insurance agencies.

Article 6. *Geographical breakdown*.

Payment service providers shall report the statistical information differentiating among:

a) domestic payment transaction;

b) cross-border payment transactions within the European Economic Area;

c) cross-border payment transactions within the European Economic Area, divided by regions according to the classification used by the *United Nations geoscheme*.

Article 7. *Recording and reference dates*.

1. The date to be considered by payment service providers for recording payment transactions and fraudulent payment transactions for the purpose of the statistical reporting is the day the transaction has been executed.

In the case of a series of transactions, the date recorded shall be the date when each individual payment transaction was executed.

2. Payment service providers shall report all fraudulent payment transactions from the time fraud has been detected (for instance: through a customer complaint or other means), regardless of whether or not the case related to the fraudulent payment transaction has been closed by the time the data are reported.

3. Payment service providers shall report all adjustments to the data referring to any past reporting period at least up to one-year-old, during the next reporting window after the information necessitating the adjustments is discovered.

To this ends, it shall be indicated that the data reported are revised figures applicable to the past period.

Article 8. *Frequency and reporting period*.

1. Payment service providers shall report the statistical information to the Financial Information Authority on annual basis, based on the applicable data breakdown(s) in the Annex.

Statistical information shall be reported with data broken down in two periods of six months.

2. Payment service providers shall report to the Financial Information Authority the statistical information on transactions registered from 1 January to 31 December of the previous year by 30 June of the following year.

Title III

Final provisions

Article 9. *Final provisions*.

1. This Instruction is without prejudice to provisions of Article 40 of the Law No. XVIII of 8 October 2013 on the reporting of suspicious activities and of Regulation No. 5 of 19 September 2018, as well as of Instruction No. 1 of 23 October 2017.

2. The Financial Information Authority updates this Instruction consistently with the development of the institutional, legal, economic, commercial and professional framework of the State, also taking into account what established by the relevant international and European bodies.

This Instruction, including the Annex, will enter into force on the day of its publication in the official web-site of the Financial Information Authority.

Vatican, 30 April 2019

RENÉ BRÜLHART
President

Visto

TOMMASO DI RUZZA
Director

Annex

Tables for statistical information on frauds related to means of payment to be reported to the Financial Information Authority

Methodological introduction

1. Payment service providers report zero («0») where there were no transactions or fraudulent transactions taking place for a particular indicator in the reporting period established. Where payment service providers cannot report data for a specific breakdown because that particular data breakdown is not applicable, the data should be reported as not applicable («NA»).

2. For the purpose of avoiding double-counting, payment service providers shall submit data in their issuing (or initiating) capacity. Data for card payments shall be reported both by the payer's payment service provider and by the payee's payment service provider acquiring the payment transaction. The two perspectives should be reported separately, with different breakdowns as detailed in this Annex. In the event that there is more than one acquiring payment service provider involved, the provider that has the contractual relationship with the payee should report. In addition, for direct debits, transactions must be reported by the payee's payment service provider only, given that these transactions are initiated by the payee.

3. In order to avoid double counting when calculating the total transactions and fraudulent transactions across all payment instruments, the payment service provider that executes credit transfers initiated by a payment initiation service provider shall indicate the breakdown for the volume and value of the total transactions and fraudulent payment transactions that have been initiated via a payment initiation service provider when reporting data breakdowns under Table A.

4. Gray cells should not be populated.

Card-based payment services

5. A payment service provider that does not manage the account of the payment service user but issues and executes card-based payments (a card-based payment instrument issuer) shall provide statistical information on volumes and values, in accordance with data breakdowns under Tables C and/or E. When such data are provided, the account service payment service provider should ensure that no double-reporting of such transactions occur.

6. The payment service provider offering credit transfer and card based payment services shall provide statistical information in accordance with data breakdowns under Tables A, C and/or D, depending on the payment instrument used for a given payment transaction and on the role of the payment service provider. The data include:

a) geographical perspective;

b) payment channel;

c) authentication method;

d) reason for not applying strong customer authentication;

e) fraud types;

f) card function for data breakdowns under Tables C and D; and

g) payment transactions initiated via a payment initiation service provider for data breakdowns under Table A.

Table A – Data breakdown for credit transfers

No.	Item	Payment transactions	Fraudulent payment transactions
1	**Credit transfers**		
1.1	Of which initiated by payment initiation service providers		
1.2	Of which initiated non-electronically		
1.3	Of which initiated electronically		
1.3.1	Of which initiated via remote payment channel		
1.3.1.1	Of which authenticated via strong customer authentication		
	of which fraudulent credit transfers by fraud types:		
1.3.1.1.1	Issuance of a payment order by the fraudster		
1.3.1.1.2	Modification of a payment order by the fraudster		
1.3.1.1.3	Manipulation of the payer by the fraudster to issue a payment order		
1.3.1.2	Of which authenticated via non-strong customer authentication		
	of which fraudulent credit transfers by fraud types:		
1.3.1.2.1	Issuance of a payment order by the fraudster		
1.3.1.2.2	Modification of a payment order by the fraudster		
1.3.1.2.3	Manipulation of the payer by the fraudster to issue a payment order		
	of which broken down by reason for authentication via non-strong customer authentication:		
1.3.1.2.4	Low value		
1.3.1.2.5	Payment to self		
1.3.1.2.6	Trusted beneficiary		
1.3.1.2.7	Recurring transaction		
1.3.1.2.8	Use of secure payment processes or protocols for legal persons		
1.3.1.2.9	Transaction risk analysis		
1.3.2	Of which initiated via non-remote payment channel		
1.3.2.1	Of which authenticated via strong customer authentication		
	of which fraudulent credit transfers by fraud types:		
1.3.2.1.1	Issuance of a payment order by the fraudster		
1.3.2.1.2	Modification of a payment order by the fraudster		
1.3.2.1.3	Manipulation of the payer by the fraudster to issue a payment order		
1.3.2.2	Of which authenticated via non-strong customer authentication		
	of which fraudulent credit transfers by fraud types:		
1.3.2.2.1	Issuance of a payment order by the fraudster		

1.3.2.2.2	Modification of a payment order by the fraudster		
1.3.2.2.3	Manipulation of the payer by the fraudster to issue a payment order		
	of which broken down by reason for non-strong customer authentication:		
1.3.1.2.4	Payment to self		
1.3.1.2.5	Trusted beneficiary		
1.3.1.2.6	Recurring transaction		
1.3.1.2.7	Contactless low value		
1.3.1.2.8	Unattended terminal for transport or parking fares		

Losses due to fraud per liability bearer	**Total losses**
The reporting payment service provider	
The Payment service user (payer)	
Others	

Validation

a) 1.2 + 1.3 = 1

b) 1.1 does not equate 1 but is a subset of 1

c) 1.3.1 + 1.3.2 = 1.3

d) 1.3.1.1 + 1.3.1.2 = 1.3.1

e) 1.3.2.1 + 1.3.2.2 = 1.3.2

f) 1.3.1.1.1 + 1.3.1.1.2 + 1.3.1.1.3 = fraudulent payment transaction figure of 1.3.1.1

g) 1.3.1.2.1 + 1.3.1.2.2 + 1.3.1.2.3 = fraudulent payment transaction figure of 1.3.1.2

h) 1.3.2.1.1 + 1.3.2.1.2 + 1.3.2.1.3 = fraudulent payment transaction figure of 1.3.2.1

i) 1.3.2.2.1 + 1.3.2.2.2 + 1.3.2.2.3 = fraudulent payment transaction figure of 1.3.2.2

j) 1.3.1.2.4 + 1.3.1.2.5 + 1.3.1.2.6 + 1.3.1.2.7 + 1.3.1.2.8 + 1.3.1.2.9 = 1.3.1.2

k) 1.3.2.2.4 + 1.3.2.2.5 + 1.3.2.2.6 + 1.3.2.2.7 + 1.3.2.2.8 = 1.3.2.2

Note

The payment service provider shall provide statistical information in accordance with data breakdowns under Table A for all payment transactions and fraudulent payment transactions executed using credit transfers.

Table B – Data breakdown for direct debits

No.	Item	Payment transactions	Fraudulent payment transactions
2	**Direct debits**		
2.1	Of which consent given via an electronic mandate		
	of which fraudulent direct debits by fraud type:		
2.1.1.1	Unauthorised payment transactions		
2.1.1.2	Manipulation of the payer by the fraudster to consent to a direct debit		
2.2	Of which consent given in another form than an electronic mandate		
	of which fraudulent direct debits by fraud type:		
2.2.1.1	Unauthorised payment transactions		
2.2.1.2	Manipulation of the payer by the fraudster to consent to a direct debit		

Losses due to fraud per liability bearer	Total losses
The reporting payment service provider	
The Payment service user (payer)	
Others	

Validation

a) 2.1 + 2.2 = 2

b) 2.1.1.1 + 2.1.1.2 = fraudulent payment transaction figure of 2.1

c) 2.2.1.1 + 2.2.1.2 = fraudulent payment transaction figure of 2.2

Note

The payment service provider shall provide statistical information in accordance with data breakdowns under Table B for all payment transactions and fraudulent payment transactions executed using direct debits. The data include:

a) geographical perspective;

b) channel used for the consent to be given; and

c) fraud types.

Table C – Data breakdown for card-based payment transactions to be reported by the issuer's payment service provider

No.	Item	Payment transactions	Fraudulent payment transactions
3	**Card payments (except cards with an e-money function only)**		
3.1	Of which initiated non-electronically		
3.2	Of which initiated electronically		
3.2.1	Of which initiated via remote payment channel		
	of which broken down by card function:		
3.2.1.1.1	Payments with cards with a debit function		
3.2.1.1.2	Payments with cards with a credit or delayed debit function		
3.2.1.2	Of which authenticated via strong customer authentication		
	of which fraudulent card payments by fraud types:		
3.2.1.2.1	Issuance of a payment order by a fraudster		
3.2.1.2.1.1	Lost or stolen card		
3.2.1.2.1.2	Card not received		
3.2.1.2.1.3	Counterfeit card		
3.2.1.2.1.4	Card details theft		
3.2.1.2.1.5	Other		
3.2.1.2.2	Modification of a payment order by the fraudster		
3.2.1.2.3	Manipulation of the payer to make a card payment		
3.2.1.3	Of which Authenticated via non-strong customer authentication		
	of which fraudulent card payments by fraud types:		
3.2.1.3.1	Issuance of a payment order by a fraudster		
3.2.1.3.1.1	Lost or stolen card		
3.2.1.3.1.2	Card not received		
3.2.1.3.1.3	Counterfeit card		
3.2.1.3.1.4	Card details theft		
3.2.1.3.1.5	Other		
3.2.1.3.2	Modification of a payment order by the fraudster		
3.2.1.3.3	Manipulation of the payer to make a card payment		
	of which broken down by reason for non-strong customer authentication		
3.2.1.3.4	Low value		
3.2.1.3.5	Payment to self		
3.2.1.3.6	Trusted beneficiary		
3.2.1.3.7	Recurring transaction		
3.2.1.3.8	Use of secure payment processes or protocols for legal persons		
3.2.2	Of which initiated via non-remote payment channel		
	of which broken down by card function:		

3.2.2.1.1	Payments with cards with a debit function		
1.3.2.1.2	Payments with cards with a credit or delayed debit function		
3.2.2.2	Of which authenticated via strong customer authentication		
	of which fraudulent card payments by fraud types:		
3.2.2.2.1	Issuance of a payment order by a fraudster		
3.2.2.2.1.1	Lost or stolen card		
3.2.2.2.1.2	Card not received		
3.2.2.2.1.3	Counterfeit card		
3.2.2.2.1.4	Card details theft		
3.2.2.2.1.5	Other		
3.2.2.2.2	Modification of a payment order by the fraudster		
3.2.2.2.3	Manipulation of the payer to make a card payment		
3.2.2.3	Of which authenticated via non-strong customer authentication		
	of which fraudulent card payments by fraud types:		
3.2.2.3.1	Issuance of a payment order by a fraudster		
3.2.2.3.1.1	Lost or stolen card		
3.2.2.3.1.2	Card not received		
3.2.2.3.1.3	Counterfeit card		
3.2.2.3.1.4	Card details theft		
3.2.2.3.2	Other		
3.2.2.3.3	Modification of a payment order by the fraudster		
	of which broken down by reason for non-strong customer authentication		
3.2.2.3.4	Trusted beneficiary		
3.2.2.3.5	Recurring transaction		
3.2.2.3.6	Contactless low value		
3.2.2.3.7	Unattended terminal for transport or parking fares		

Losses due to fraud per liability bearer	**Total losses**
The reporting payment service provider	
The Payment service user (payer)	
Others	

Validation

a) 3.1 + 3.2 = 3

b) 3.2.1 + 3.2.2 = 3.2

c) 3.2.1.1.1 + 3.2.1.1.2 = 3.2.1

d) 3.2.2.1.1 + 3.2.2.1.2 = 3.2.2

e) 3.2.1.2 + 3.2.1.3 = 3.2.1

f) 3.2.2.2 + 3.2.2.3 = 3.2.2

g) 3.2.1.2.1 + 3.2.1.2.2 + 3.2.1.2.3 = fraudulent payment transaction figure of 3.2.1.2

h) 3.2.1.3.1 + 3.2.1.3.2 + 3.2.1.3.3 = fraudulent payment transaction figure of 3.2.1.3

i) 3.2.2.2.1 + 3.2.2.2.2 + 3.2.2.2.3 = fraudulent payment transaction figure of 3.2.2.2

j) 3.2.2.3.1 + 3.2.2.3.2 + 3.2.2.3.3 = fraudulent payment transaction figure of 3.2.2.3

k) 3.2.1.2.1.1 + 3.2.1.2.1.2 + 3.2.1.2.1.3 + 3.2.1.2.1.4 + 3.2.1.2.1.5 = fraudulent payment transaction figure of 3.2.1.2.1

l) 3.2.1.3.1.1 + 3.2.1.3.1.2 + 3.2.1.3.1.3 + 3.2.1.3.1.4 + 3.2.1.3.1.5 = fraudulent payment transaction figure of 3.2.1.3.1

m) 3.2.2.2.1.1 + 3.2.2.2.1.2 + 3.2.2.2.1.3 + 3.2.2.2.1.4 = fraudulent payment transaction figure of 3.2.2.2.1

n) 3.2.2.3.1.1 + 3.2.2.3.1.2 + 3.2.2.3.1.3 + 3.2.2.3.1.4 = fraudulent payment transaction figure of 3.2.2.3.1

o) 3.2.1.3.4 + 3.2.1.3.5 + 3.2.1.3.6 + 3.2.1.3.7 + 3.2.1.3.8 = 3.2.1.3

p) 3.2.2.3.4 + 3.2.2.3.5 + 3.2.2.3.6 + 3.2.2.3.7 = 3.2.2.3

Note

The payment service provider shall provide statistical information in accordance with data breakdowns under Table C for all payment transactions and fraudulent payment transactions on the issuer side where a payment card was used and the payment service provider was the payer’s payment service provider.

The payment service provider reporting card payment transactions in accordance with data breakdowns under Table C shall exclude cash withdrawals and cash deposits.

Table D – Data breakdown for card-based payments transactions to be reported by the acquirer's payment service provider (with a contractual relationship with the payment service user)

No.	Item	Payment transactions	Fraudulent payment transactions
4	**Card payments acquired (except cards with an e-money function only)**		
4.1	Of which initiated non-electronically		
4.2	Of which initiated electronically		
4.2.1	Of which acquired via a Remote channel		
	of which broken down by card function:		
4.2.1.1.1	Payments with cards with a debit function		
4.2.1.1.2	Payments with cards with a credit or delayed debit function		
4.2.1.2	Of which authenticated via strong customer authentication		
	of which fraudulent card payments by fraud types:		
4.2.1.2.1	Issuance of a payment order by a fraudster		
4.2.1.2.1.1	Lost or stolen card		
4.2.1.2.1.2	Card not received		
4.2.1.2.1.3	Counterfeit card		
4.2.1.2.1.4	Card details theft		
4.2.1.2.1.5	Other		
4.2.1.2.2	Modification of a payment order by the fraudster		
4.2.1.2.3	Manipulation of the payer to make a card payment		
4.2.1.3	Of which authenticated via non-strong customer authentication		
	of which fraudulent card payments by fraud types:		
4.2.1.3.1	Issuance of a payment order by a fraudster		
4.2.1.3.1.1	Lost or stolen card		
4.2.1.3.1.2	Card not received		
4.2.1.3.1.3	Counterfeit card		
4.2.1.3.1.4	Card details theft		
4.2.1.3.1.5	Other		
4.2.1.3.2	Modification of a payment order by the fraudster		
4.2.1.3.3	Manipulation of the payer to make a card payment		
	of which broken down by reason for non-strong customer authentication		
4.2.1.3.4	Low value		
4.2.1.3.5	Recurring transaction		
3.2.1.3.6	Transaction risk analysis		
4.2.2	Of which acquired via a non-remote channel		
	of which broken down by card function:		
4.2.2.1.1	Payments with cards with a debit function		
4.3.2.1.2	Payments with cards with a credit or delayed debit function		

4.2.2.2	Of which Authenticated via strong customer authentication		
	of which fraudulent card payments by fraud types:		
4.2.2.2.1	Issuance of a payment order by a fraudster		
4.2.2.2.1.1	Lost or stolen card		
4.2.2.2.1.2	Card not received		
4.2.2.2.1.3	Counterfeit card		
4.2.2.2.1.4	Other		
4.2.2.2.2	Modification of a payment order by the fraudster		
4.2.2.2.3	Manipulation of the payer to make a card payment		
4.2.2.3	Of which authenticated via non-strong customer authentication		
	of which fraudulent card payments by fraud types:		
4.2.2.3.1	Issuance of a payment order by a fraudster		
4.2.2.3.1.1	Lost or stolen card		
4.2.2.3.1.2	Card not received		
4.2.2.3.1.3	Counterfeit card		
4.2.2.3.1.4	Other		
4.2.2.3.2	Modification of a payment order by the fraudster		
4.2.2.3.3	Manipulation of the payer to make a card payment		
	of which broken down by reason for non-strong customer authentication:		
4.2.2.3.4	Recurring transaction		
4.2.2.3.5	Contactless low value		
4.2.2.3.6	Unattended terminal for transport or parking fares		

Losses due to fraud per liability bearer	**Total losses**
The reporting payment service provider	
The Payment service user (payer)	
Others	

Validation

a) 4.1 + 4.2 = 4

b) 4.2.1 + 4.2.2 = 4.2

c) 4.2.1.1.1 + 4.2.1.1.2 = 4.2.1

d) 4.2.2.1.1 + 4.2.2.1.2 = 4.2.2

e) 4.2.1.2 + 4.2.1.3 = 4.2.1

f) 4.2.2.2 + 4.2.2.3 = 4.2.2

g) 4.2.1.2.1 + 4.2.1.2.2 + 4.2.1.2.3 = fraudulent payment transaction figure of 4.2.1.2

h) 4.2.1.3.1 + 4.2.1.3.2 + 4.2.1.3.3 = fraudulent payment transaction figure of 4.2.1.3

i) 4.2.2.2.1 + 4.2.2.2.2 + 4.2.2.2.3 = fraudulent payment transaction figure of 4.2.2.2

j) 4.2.2.3.1 + 4.2.2.3.2 + 4.2.2.3.3 = fraudulent payment transaction figure of 4.2.2.3

k) 4.2.1.2.1.1 + 4.2.1.2.1.2 + 4.2.1.2.1.3 + 4.2.1.2.1.4 + 4.2.1.2.1.5 = fraudulent payment transaction figure of 4.2.1.2.1

l) 4.2.1.3.1.1 + 4.2.1.3.1.2 + 4.2.1.3.1.3 + 4.2.1.3.1.4 + 4.2.1.3.1.5 = fraudulent payment transaction figure of 4.2.1.3.1

m) 4.2.2.2.1.1 + 4.2.2.2.1.2 + 4.2.2.2.1.3 + 4.2.2.2.1.4 = fraudulent payment transaction figure of 4.2.2.2.1

n) 4.2.2.3.1.1 + 4.2.2.3.1.2 + 4.2.2.3.1.3 + 4.2.2.3.1.4 = fraudulent payment transaction figure of 4.2.2.3.1

o) 4.2.1.3.4 + 4.2.1.3.5 + 4.2.1.3.6 + = 4.2.1.3

p) 4.2.2.3.4 + 4.2.2.3.5+ 4.2.2.3.6 = 4.2.2.3

Note

The payment service provider shall provide statistical information in accordance with data breakdown under Table D for all payment transactions and fraudulent payment transactions on the acquiring side where a payment card was used and the payment service provider is the payee’s payment service provider.

The payment service provider reporting card payment transactions in accordance with data breakdowns under Table D shall exclude cash withdrawals and cash deposits.

Table E – Data Breakdown for cash withdrawals using cards to be reported by the card issuer's payment service provider

No.	Item	Payment transactions	Fraudulent payment transactions
5	**Cash withdrawals**		
	Of which broken down by card function		
5.1	Of which payments with cards with a debit function		
5.2	Of which payments with cards with a credit or delayed debit function		
	of which fraudulent card payments by fraud types:		
5.2.1	Issuance of a payment order (cash withdrawal) by the fraudster		
5.2.1.1	Lost or stolen card		
5.2.1.2	Card not received		
5.2.1.3	Counterfeit card		
5.2.1.4	Other		
5.2.2	Manipulation of the payer to make a cash withdrawal		

Losses due to fraud per liability bearer	Total losses
The reporting payment service provider	
The Payment service user (payer)	
Others	

Validation

a) 5.1 + 5.2 = 5

b) 5.2.1 + 5.2.2 = 5

c) 5.2.1.1 + 5.2.1.2 + 5.2.1.3 + 5.2.1.4 = 5.2.1

Note

The payment service provider (issuer) shall provide statistical information in accordance with data breakdowns under Table E for all cash withdrawals and fraudulent cash withdrawals through apps, at ATMs, at bank counters and through retailers ('cash back') using a card.

Table F – Data Breakdown to be provided for e-money payment transactions

No.	Item	Payment transactions	Fraudulent payment transactions
6	**E-money payment transactions**		
6.1	Of which via remote payment initiation channel		
6.1.1	Of which authenticated via strong customer authentication		
	of which fraudulent e-money payment transactions by fraud types:		
6.1.1.1	Issuance of a payment order by the fraudster		
6.1.1.2	Modification of a payment order by the fraudster		
6.1.1.3	Manipulation of the payer by the fraudster to issue a payment order		
6.1.2	Of which authenticated via non-strong customer authentication		
	of which fraudulent e-money payment transactions by fraud types:		
6.1.2.1	Issuance of a payment order by the fraudster		
6.1.2.2	Modification of a payment order by the fraudster		
6.1.2.3	Manipulation of the payer by the fraudster to issue a payment order		
	of which broken down by reason for non-strong customer authentication		
6.1.2.4	Low value		
6.1.2.5	Trusted beneficiary		
6.1.2.6	Recurring transaction		
6.1.2.7	Payment to self		
6.1.2.8	Use of secure payment processes or protocols for legal persons		
6.1.2.9	Transaction risk analysis		
6.2	Of which via non-remote payment initiation channel		
6.2.1	Of which authenticated via strong customer authentication		
	of which fraudulent e-money payment transactions by fraud types:		
6.2.1.1	Issuance of a payment order by the fraudster		
6.2.1.2	Modification of a payment order by the fraudster		
6.2.1.3	Manipulation of the payer by the fraudster to issue a payment order		
6.2.2	Of which authenticated via non-strong customer authentication		
	of which fraudulent e-money payment transactions by fraud types:		
6.2.2.1	Issuance of a payment order by the fraudster		
6.2.2.2	Modification of a payment order by the fraudster		
6.2.2.3	Manipulation of the payer by the fraudster to issue a payment order		
	of which broken down by reason for non-strong customer authentication		
6.2.2.4	Trusted beneficiary		
6.2.2.5	Recurring transaction		
6.2.2.6	Contactless low value		

6.2.2.7	Unattended terminal for transport or parking fares		

Losses due to fraud per liability bearer	**Total losses**
The reporting payment service provider	
The Payment service user (payer)	
Others	

Validation

a) 6.1 + 6.2 = 6

b) 6.1.1 + 6.1.2 = 6.1

c) 6.2.1 + 6.2.2 = 6.2

d) 6.1.1.1 + 6.1.1.2 + 6.1.1.3 = fraudulent payment transaction figure of 6.1.1

e) 6.1.2.1 + 6.1.2.2 + 6.1.2.3 = fraudulent payment transaction figure of 6.1.2

f) 6.2.1.1 + 6.2.1.2 + 6.2.1.3 = fraudulent payment transaction figure of 6.2.1

g) 6.2.2.1 + 6.2.2.2 + 6.2.2.3 = fraudulent payment transaction figure of 6.2.2

h) 6.1.2.4 + 6.1.2.5 + 6.1.2.6 + 6.1.2.7 + 6.1.2.8 + 6.1.2.9 = 6.1.2

i) 6.2.2.4 + 6.2.2.5 + 6.2.2.6 + 6.2.2.7 = 6.2.2

Note

1. Transactions and fraudulent transactions where e-money has been transferred by an e-money provider to a beneficiary account, including where the payer's payment service provider is identical to the payee's payment service provider, shall be reported by the e-money provider in accordance with data breakdowns under Table F.

Where the payment service providers are different, payment is only reported by the payer's payment service provider to avoid double counting.

2. When providing data on e-money transactions, the payment service provider should include e-money payment transactions

a) where the payer's payment service provider is identical to the payee's payment service provider; or

b) where a card with an e-money functionality is used.

3. The payment service provider for the purpose of e-money payment transactions should report data on volumes and values of all payment transactions, as well as volumes and values of fraudulent payment transactions, with the following breakdowns:

a) geographical perspective;

b) payment channel;

c) authentication method;

d) reason for not applying strong customer authentication (referring to the exemptions to strong customer authentication); and

e) fraud types.

Table G – Data breakdown to be provided for money remittance payment transactions

No.	Item	Payment transactions	Fraudulent payment transactions
7	**Money remittances**		

Note

1. In the case of money remittance services where funds were transferred from a payer's payment service provider to a payer's money remitter payment service provider (as part of a money remittance payment transaction), it is the payer's payment service provider, rather than the money remitter payment service provider, who shall report the payment transactions from the payer's payment service provider to the money remitter.

Such transactions shall not be reported by the payment service provider of the beneficiary of the money remittance payment transaction.

2. Transactions and fraudulent transactions where funds have been transferred by a money remitter payment service provider from its accounts to a beneficiary account, including through arrangements offsetting the value of multiple transactions (netting arrangements), shall be reported by the money remitter payment service provider in accordance with data breakdowns under Table G.

3. For money remittance services, the payment service provider shall report statistical information on volumes and values of all payment transactions and fraudulent payment transactions with the geographical perspective.

Table H – Data breakdown for transactions initiated by payment initiation services providers

No.	Item	Payment transactions	Fraudulent payment transactions
8	**Payment transactions initiated by payment initiation service providers**		
8.1	Of which initiated via remote payment channel		
8.1.1	Of which authenticated via strong customer authentication		
8.1.2	Of which authenticated via non-strong customer authentication		
8.2	Of which initiated via non-remote payment channel		
8.2.1	Of which authenticated via strong customer authentication		
8.2.2	Of which authenticated via non-strong customer authentication		
	of which broken down by payment instrument		
8.3.1	Credit transfers		
8.3.2	Other		

Validation

a) 8.1 + 8.2 = 8

b) 8.3.1 + 8.3.2 = 8

c) 8.1.1 + 8.1.2 = 8.1

d) 8.2.1 + 8.2.2 = 8.2

Note

1. When providing provides payment initiation services, the payment service provider shall provide statistical information in accordance with data breakdowns under Table H. The payment service provider shall report the executed payment transactions it initiated and the executed fraudulent transactions it initiated, both by volume and value.

2. For those payment transactions that qualify for data breakdowns under Table H, the payment service provider offering payment initiation services shall record and report data on volumes and values with the following breakdowns:

a) geographical perspective;

b) payment instrument;

c) payment channel; and

d) authentication method.