Payment Fraud Reporting Regulation

(ZBMV; Zahlungsbetrugsmeldeverordnung)

Full title

Regulation of the Financial Market Authority (FMA) on statistical reporting of cases of fraud by payment service providers (ZBMV; Zahlungsbetrugsmeldeverordnung)

Original Version: Federal Law Gazette II No. 219/2022

Preamble/Promulgation clause

Based on Article 86 para 4 of the Payment Services Act 2018 (ZaDiG 2018, Zahlungsdienstegesetz 2018), published in Federal Law Gazette I no. 17/2018, last amended by Federal Act in Federal Law Gazette I no. 36/2022, the following shall be determined by Regulation with the consent of the Federal Minister of Finance:

Text

Reporting Requirements

Article 1 (1) Payment service providers shall submit reports in accordance with this Regulation about statistical data about cases of fraud in relation to the various instruments of payment pursuant to Article 86 para. 3 of the Payment Services Act 2018; (ZaDiG 2018; Zahlungsdienstegesetz), published in Federal Law Gazette I No. 17/2018, in the version amended by federal act in Federal Law Gazette I No. 36/2022.

(2) Reports pursuant to para. 1 shall be submitted semi-annually with the reporting dates 30 June and 31 December, and shall be submitted exclusively to the Oesterreichische Nationalbank (OeNB) at latest two months after the respective reporting date.

(3) The content and specific format of the reports pursuant to para. 1 shall correspond with that of the **Annex**.

(4) Where the payment service provider is required to submit reports on payment transactions statistics pursuant to Section 5 of the Data Model Regulation 2018 (Datenmodellverordnung 2018), published in Federal Law Gazette II No. 182/2018, in the version of the Regulation amended in Federal Law Gazette II No. 548/2021, then by making that report to the OeNB in an orderly and complete manner, then the reporting obligation for the respective reporting period pursuant to para. 1 shall also be fulfilled.

Entry into force

Article 2 This Federal Act shall enter into force on the following day after publication. Reporting in accordance with this Regulation shall be made for the first time with reporting date of 30 June 2022.

to the Regulation of the Financial Market Authority (FMA) on statistical reporting of cases of fraud by payment service providers (Payment Fraud Reporting Regulation (ZBMV; Zahlungsbetrugsmeldeverordnung))[1]

A.   Data breakdown for credit transfers

	Items	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	xxx	
1.3.1.1.2	Modification of a payment order by the fraudster	xxx	
1.3.1.1.3	Manipulation of the payer by the fraudster to issue a payment order	xxx	
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	xxx	
1.3.1.2.2	Modification of a payment order by the fraudster	xxx	
1.3.1.2.3	Manipulation of the payer by the fraudster to issue a payment order	xxx	
of which broken down by reason for authentication via non-strong customer authentication			

---

[1] To fill this annex, the quantity of transactions during the reporting period is to be stated in the respective reporting fields. Unless stated otherwise in the annex, amounts in euro cents and percentages are to be indicated precisely to two decimal places. In so doing, the following digit shall be rounded down if between one and four, and rounded up if between five and nine.

1.3.1.2.4	Low value (Article 16 RTS[2])		
1.3.1.2.5	Credit transfers between accounts held by the same natural or legal person (Article 15 RTS)		
1.3.1.2.6	Trusted beneficiary (Article 13 RTS)		
1.3.1.2.7	Recurring transactions (Article 14 RTS)		
1.3.1.2.8	Use of secure corporate payment processes or protocols (Article 17 RTS)		
1.3.1.2.9	Transaction risk analysis (Article 18 RTS)		
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	xxx	
1.3.2.1.2	Modification of a payment order by the fraudster	xxx	
1.3.2.1.3	Manipulation of the payer by the fraudster to issue a payment order	xxx	
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	xxx	
1.3.2.2.2	Modification of a payment order by the fraudster	xxx	
1.3.2.2.3	Manipulation of the payer by the fraudster to issue a payment order	xxx	
of which broken down by reason for non-strong customer authentication			
1.3.2.2.4	Credit transfers between accounts held by the same natural or legal person (Article 15 RTS)		
1.3.2.2.5	Trusted beneficiary (Article 13 RTS)		

---

[2] Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to product oversight and governance requirements for insurance undertakings and insurance distributors, OJ L 69, 13.03.2018, p. 23.

1.3.2.2.6	Recurring transactions (Article 14 RTS)		
1.3.2.2.7	Contactless payments at the point of sale (Article 11 RTS)		
1.3.2.2.8	Unattended terminals for transport fares and parking fees (Article 12 RTS)		

Losses due to fraud by liability bearer:	Total losses
The reporting payment service provider	
The payment service user (payer)	
Other	

Validation

1.2 + 1.3 = 1; 1.1 does not equal 1, but is a subamount of 1
1.3.1 + 1.3.2 = 1.3
1.3.1.1 + 1.3.1.2 = 1.3.1
1.3.2.1 + 1.3.2.2 = 1.3.2
1.3.1.1.1 + 1.3.1.1.2 + 1.3.1.1.3 = Total of fraudulent payment transactions in 1.3.1.1; 1.3.1.2.1 + 1.3.1.2.2 + 1.3.1.2.3 = Total of fraudulent payment transactions in 1.3.1.2; 1.3.2.1.1 + 1.3.2.1.2 + 1.3.2.1.3 = Total of fraudulent payment transactions in 1.3.2.1; 1.3.2.2.1 + 1.3.2.2.2 + 1.3.2.2.3 = Total of fraudulent payment transactions in 1.3.2.2
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
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

B.   Data breakdown for direct debits

	Items	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 types:			
2.1.1.1	Unauthorised payment transactions	xxx	
2.1.1.2	Manipulation of the payer by the fraudster to receive consent to a direct debit	xxx	
2.2	Of which consent given in another form than an electronic mandate	xxx	
of which fraudulent direct debits by fraud types:			
2.2.1.1	Unauthorised payment transactions	xxx	
2.2.1.2	Manipulation of the payer by the fraudster to receive consent to a direct debit	xxx	

Losses due to fraud by liability bearer:	Total losses
The reporting payment service provider	
The payment service user (payer)	
Other	

Validation

2.1 + 2.2 = 2
2.1.1.1 + 2.1.1.2 = Value of fraudulent payment transactions in 2.1
2.2.1.1 + 2.2.1.2 = Value of fraudulent payment transactions in 2.2

C. Data breakdown for card-based payment transactions to be reported by the issuing payment service provider

	Items	Payment transactions	Fraudulent payment transactions
3	**Card payments (via cards only with an e-money function)**		
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 the fraudster	xxx	
3.2.1.2.1.1	Lost or stolen card	xxx	
3.2.1.2.1.2	Card not received	xxx	
3.2.1.2.1.3	Counterfeit card	xxx	
3.2.1.2.1.4	Card details theft	xxx	
3.2.1.2.1.5	Other issues	xxx	
3.2.1.2.2	Modification of a payment order by the fraudster	xxx	
3.2.1.2.3	Manipulation of the payer to make a card payment	xxx	
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 the fraudster	xxx	
3.2.1.3.1.1	Lost or stolen card	xxx	
3.2.1.3.1.2	Card not received	xxx	
3.2.1.3.1.3	Counterfeit card	xxx	
3.2.1.3.1.4	Card details theft	xxx	
3.2.1.3.1.5	Other issues	xxx	

3.2.1.3.2	Modification of a payment order by the fraudster	xxx	
3.2.1.3.3	Manipulation of the payer to make a card payment	xxx	
of which broken down by reason for non-strong customer authentication			
3.2.1.3.4	Low value (Article 16 RTS)		
3.2.1.3.5	Trusted beneficiary (Article 13 RTS)		
3.2.1.3.6	Recurring transactions (Article 14 RTS)		
3.2.1.3.7	Use of secure corporate payment processes or protocols (Article 17 RTS)		
3.2.1.3.8	Transaction risk analysis (Article 18 RTS)		
3.2.1.3.9	Merchant initiated transactions		
3.2.1.3.10	Other issues		
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		
3.2.2.1.2	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 the fraudster	xxx	
3.2.2.2.1.1	Lost or stolen card	xxx	
3.2.2.2.1.2	Card not received	xxx	
3.2.2.2.1.3	Counterfeit card	xxx	
3.2.2.2.1.4	Other issues	xxx	
3.2.2.2.2	Modification of a payment order by the fraudster	xxx	
3.2.2.2.3	Manipulation of the payer to make a card payment	xxx	
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 the fraudster	xxx	
3.2.2.3.1.1	Lost or stolen card	xxx	
3.2.2.3.1.2	Card not received	xxx	
3.2.2.3.1.3	Counterfeit card	xxx	
3.2.2.3.1.4	Other issues	xxx	
3.2.2.3.2	Modification of a payment order by the fraudster	xxx	
3.2.2.3.3	Manipulation of the payer to make a card payment	xxx	
of which broken down by reason for non-strong customer authentication:			
3.2.2.3.4	Trusted beneficiary (Article 13 RTS)		
3.2.2.3.5	Recurring transactions (Article 14 RTS)		
3.2.2.3.6	Contactless low value (Article 11 RTS)		
3.2.2.3.7	Unattended terminal for transport fares and parking fees (Article 12 RTS)		
3.2.2.3.8	Other issues		

Losses due to fraud by liability bearer:	Total losses
The reporting payment service provider	
The payment service user (payer)	
Other	

Validation

3.1 + 3.2 = 3
3.2.1 + 3.2.2 = 3.2
3.2.1.1.1 + 3.2.1.1.2 = 3.2.1; 3.2.2.1.1 + 3.2.2.1.2 = 3.2.2
3.2.1.2 + 3.2.1.3 = 3.2.1; 3.2.2.2 + 3.2.2.3 = 3.2.2
3.2.1.2.1 + 3.2.1.2.2 + 3.2.1.2.3 = Total of fraudulent payment transactions in 3.2.1.2; 3.2.1.3.1 + 3.2.1.3.2 + 3.2.1.3.3 = Total of fraudulent payment transactions in 3.2.1.3; 3.2.2.2.1 + 3.2.2.2.2 + 3.2.2.2.3 = Total of fraudulent payment transactions in 3.2.2.2; 3.2.2.3.1 + 3.2.2.3.2 + 3.2.2.3.3 = 3.2.2.3
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 = Total of fraudulent payment transactions in 3.2.1.2.1; 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 = Total of fraudulent payment transactions in 3.2.1.3.1; 3.2.2.2.1.1 + 3.2.2.2.1.2 + 3.2.2.2.1.3 + 3.2.2.2.1.4 = Total of fraudulent payment transactions in 3.2.2.2.1; 3.2.2.3.1.1 + 3.2.2.3.1.2 + 3.2.2.3.1.3 + 3.2.2.3.1.4 = 3.2.2.3.1
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; 3.2.2.3.4 + 3.2.2.3.5 + 3.2.2.3.6 + 3.2.2.3.7 = 3.2.2.3

D. **Data breakdown for card-based payment transactions to be reported by the acquiring payment service provider (with a contractual relationship with the payment service user)**

	Items	Payment transactions	Fraudulent payment transactions
4	**Card payments acquired (via cards only with an e-money function)**		
4.1	Of which initiated non-electronically		
4.2	Of which initiated electronically		
4.2.1	Of which acquired by 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 the fraudster	xxx	
4.2.1.2.1.1	Lost or stolen card	xxx	
4.2.1.2.1.2	Card not received	xxx	
4.2.1.2.1.3	Counterfeit card	xxx	
4.2.1.2.1.4	Card details theft	xxx	
4.2.1.2.1.5	Other issues	xxx	
4.2.1.2.2	Modification of a payment order by the fraudster	xxx	
4.2.1.2.3	Manipulation of the payer to make a card payment	xxx	
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 the fraudster	xxx	
4.2.1.3.1.1	Lost or stolen card	xxx	
4.2.1.3.1.2	Card not received	xxx	
4.2.1.3.1.3	Counterfeit card	xxx	
4.2.1.3.1.4	Card details theft	xxx	

4.2.1.3.1.5	Other issues	xxx	
4.2.1.3.2	Modification of a payment order by the fraudster	xxx	
4.2.1.3.3	Manipulation of the payer to make a card payment	xxx	
of which broken down by reason for non-strong customer authentication:			
4.2.1.3.4	Low value (Article 16 RTS)		
4.2.1.3.5	Recurring transactions (Article 14 RTS)		
4.2.1.3.6	Transaction risk analysis (Article 18 RTS)		
4.2.1.3.7	Merchant initiated transactions		
4.2.1.3.8	Other issues		
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		
4.2.2.1.2	Payments with cards with a credit or "delayed" debit function		
4.2.2.2	**Of which authenticated non-strong customer authentication**		
of which fraudulent card payments by fraud types:			
4.2.2.2.1	Issuance of a payment order by the fraudster	xxx	
4.2.2.2.1.1	Lost or stolen card	xxx	
4.2.2.2.1.2	Card not received	xxx	
4.2.2.2.1.3	Counterfeit card	xxx	
4.2.2.2.1.4	Other issues	xxx	
4.2.2.2.2	Modification of a payment order by the fraudster	xxx	
4.2.2.2.3	Manipulation of the payer to make a card payment	xxx	
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 the fraudster	xxx	
4.2.2.3.1.1	Lost or stolen card	xxx	
4.2.2.3.1.2	Card not received	xxx	

4.2.2.3.1.3	Counterfeit card	xxx	
4.2.2.3.1.4	Other issues	xxx	
4.2.2.3.2	Modification of a payment order by the fraudster	xxx	
4.2.2.3.3	Manipulation of the payer to make a card payment	xxx	
of which broken down by reason for non-strong customer authentication:			
4.2.2.3.4	Recurring transactions (Article 14 RTS)		
4.2.2.3.5	Contactless low value (Article 11 RTS)		
4.2.2.3.6	Unattended terminals for transport fares and parking fees (Article 12 RTS)		
4.2.2.3.7	Other issues		

Losses due to fraud by liability bearer:	Total losses
The reporting payment service provider	
The payment service user (payer)	
Other	

Validation

4.1 + 4.2 = 4
4.2.1 + 4.2.2 = 4.2
4.2.1.1.1 + 4.2.1.1.2 = 4.2.1; 4.2.2.1.1 + 4.2.2.1.2 = 4.2.2
4.2.1.2 + 4.2.1.3 = 4.2.1; 4.2.2.2 + 4.2.2.3 = 4.2.2
4.2.1.2.1 + 4.2.1.2.2 + 4.2.1.2.3 = Number of fraudulent payment transactions reported 4.2.1.2; 4.2.1.3.1 + 4.2.1.3.2 + 4.2.1.3.3 = Number of fraudulent payment transactions reported 4.2.1.3; 4.2.2.2.1 + 4.2.2.2.2 + 4.2.2.2.3 = Number of fraudulent payment transactions reported 4.2.2.2; 4.2.2.3.1 + 4.2.2.3.2 + 4.2.2.3.3 = 4.2.2.3
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 = Number of fraudulent payment transactions reported 4.2.1.2.1; 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 = Number of fraudulent payment transactions reported 4.2.1.3.1; 4.2.2.2.1.1 + 4.2.2.2.1.2 + 4.2.2.2.1.3 + 4.2.2.2.1.4 = Number of fraudulent payment transactions reported 4.2.2.2.1; 4.2.2.3.1.1 + 4.2.2.3.1.2 + 4.2.2.3.1.3 + 4.2.2.3.1.4 = 4.2.2.3.1
4.2.1.3.4 + 4.2.1.3.5 + 4.2.1.3.6 = 4.2.1.3; 4.2.2.3.4 + 4.2.2.3.5 + 4.2.2.3.6 = 4.2.2.3

E. **Data breakdown for cash withdrawals using cards to be reported by the card issuing payment service provider**

	Items	Payment transactions	Fraudulent payment transactions
5	**Cash withdrawals**		
of which broken down by card function:			
5.1	Of which cash withdrawals with cars with a debit function		
5.2	Of which cash withdrawals with cards with a credit or "delayed" debit function		
of which fraudulent cash withdrawals by fraud types:			
5.2.1	Issuance of a payment order (cash withdrawal) by the fraudster	xxx	
5.2.1.1	Lost or stolen card	xxx	
5.2.1.2	Card not received	xxx	
5.2.1.3	Counterfeit card	xxx	
5.2.1.4	Other issues	xxx	
5.2.2	Manipulation of the payer to make a cash withdrawal	xxx	

Losses due to fraud by liability bearer:	Total losses
The reporting payment service provider	
The payment service user (payer)	
Other	

Validation

5.1 + 5.2 = 5
5.2.1 + 5.2.2 = 5
5.2.1.1 + 5.2.1.2 + 5.2.1.3 + 5.2.1.4 = 5.2.1

F. Data breakdown to be provided for e-money payment transactions

	Items	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	xxx	
6.1.1.2	Modification of a payment order by the fraudster	xxx	
6.1.1.3	Manipulation of the payer by the fraudster to issue a payment order	xxx	
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	xxx	
6.1.2.2	Modification of a payment order by the fraudster	xxx	
6.1.2.3	Manipulation of the payer by the fraudster to issue a payment order	xxx	
of which broken down by reason for non-strong customer authentication:			
6.1.2.4	Low value (Article 16 RTS)		
6.1.2.5	Trusted beneficiary (Article 13 RTS)		
6.1.2.6	Recurring transactions (Article 14 RTS)		
6.1.2.7	Payment to self (Article 15 RTS)		
6.1.2.8	Use of secure corporate payment processes or protocols (Article 17 RTS)		
6.1.2.9	Transaction risk analysis (Article 18 RTS)		
6.1.2.10	Merchant initiated transactions		
6.1.2.11	Other issues		
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	xxx	
6.2.1.2	Modification of a payment order by the fraudster	xxx	
6.2.1.3	Manipulation of the payer by the fraudster to issue a payment order	xxx	
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	xxx	
6.2.2.2	Modification of a payment order by the fraudster	xxx	
6.2.2.3	Manipulation of the payer by the fraudster to issue a payment order	xxx	
of which broken down by reason for non-strong customer authentication:			
6.2.2.4	Trusted beneficiary (Article 13 RTS)		
6.2.2.5	Recurring transactions (Article 14 RTS)		
6.2.2.6	Contactless low value (Article 11 RTS)		
6.2.2.7	Unattended terminals for transport fares and parking fees (Article 12 RTS)		
6.2.2.8	Other issues		

Losses due to fraud by liability bearer:	Total losses
The reporting payment service provider	
The payment service user (payer)	
Other	

Validation

6.1 + 6.2 = 6
6.1.1 + 6.1.2 = 6.1; 6.2.1 + 6.2.2 = 6.2
6.1.1.1 + 6.1.1.2 + 6.1.1.3 = Number of fraudulent payment transactions reported 6.1.1; 6.1.2.1 + 6.1.2.2 + 6.1.2.3 = Number of fraudulent payment transactions reported 6.1.2; 6.2.1.1 + 6.2.1.2 + 6.2.1.3 = Number of fraudulent payment transactions reported 6.2.1; 6.2.2.1 + 6.2.2.2 + 6.2.2.3 = 6.2.2
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; 6.2.2.4 + 6.2.2.5 + 6.2.2.6 + 6.2.2.7 = 6.2.2

CAUTION: This Annex has been translated purely for information purposes and the translated version of the form is neither intended nor valid for submission.

G.   Data breakdown to be provided for money remittance payment transactions

	Items	Payment transactions	Fraudulent payment transactions
7	**Money remittance**		

H.   Data breakdown for transactions initiated by payment initiation service providers

	Items	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 issues		

Validation

8.1 + 8.2 = 8
8.3.1 + 8.3.2 = 8
8.1.1 + 8.1.2 = 8.1
8.2.1 + 8.2.2 = 8.2