Chapter 16

Reporting requirements

Notes on completing REP017 Payments Fraud Report

These notes contain guidance for payment service providers that are required to complete the Payments Fraud Report in accordance with Regulation 109(4) of the Payment Services Regulations 2017 and SUP 16.13.7D. The notes also build on the EBA Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2) (EBA/GL/2018/05) ("the EBA Guidelines").

The following completion notes should be read in conjunction with the EBA Guidelines.

Question A1 – reporting period

As per SUP16.13.8, small payment institutions, registered account information service providers and small electronic money institutions must report once per year. All other PSPs must report every six months.

Those PSPs required to report annually are required to provide separate Payment Fraud Reports in respect of the two halves of the reporting year. These PSPs should use question 1 in the Payments Fraud Report to select the period the data in their return covers, e.g. "H1" for the period covering 1 January to 30 June, and "H2" for the period covering 1 July to 31 December.

Table 1 - Payment transactions and fraudulent payment transactions for payment services

The form provides the means for PSPs to provide the FCA with statistical data on fraud related to different means of payment.

As outlined in Guideline 1 of the EBA Guidelines, PSPs will be required to collect and submit data on the volume and value of all payment transactions, as well as the volume and value of fraudulent transactions.

Data on volume and value need to be broken down further by payment type, fraud type, method of authentication and geographical location. The detailed breakdown of data to be reported generally pertains only to the volume and value of fraudulent transactions (as opposed to all payment transactions). The EBA Guidelines explain these in detail. The following completion notes should be read as complementary to the Guidelines.

Table 2 - Fraud relating to account information services

PSPs that provide account information services (AISPs) should have regard to Table 2 in the fraud report (and the guidance in table 2 below). Registered account information service providers (i.e. PSPs that do not provide any other type of payment service) do not need to answer the questions in Table 1 of the fraud report.

Adjustments

The date to be considered by PSPs for recording payment transactions and fraudulent payment transactions for the purpose of this statistical reporting is the day the transaction has been executed in accordance with PSD2.

However, payment service users are entitled to redress for unauthorised transactions as long as they have notified their PSP no later than 13 months after the debit date, on becoming aware of any unauthorised payment transactions. This means PSPs may need to adjust reports which they have already submitted, on becoming aware of fraudulent transactions executed in previous reporting periods.

Furthermore, the payment service provider should report all fraudulent payment transactions from the time fraud has been detected (i.e. because it has been reported to the PSP such as through a customer complaint or otherwise discovered independently by the PSP), regardless of whether or not the case related to the fraudulent payment transaction has been closed by the time the data are reported. This

means PSPs may need to adjust reports which they have already submitted, should investigation of open fraud cases conclude that a transaction was not fraudulent.

PSPs should report adjustments during the next reporting window after the information necessitating the adjustment is discovered.

PSPs should make use of the resubmission facility made available via the electronic means for submitting REP017.

Table 1 - What is a fraudulent transaction?

For the purposes of table 1 a fraudulent transaction is any payment transaction that the PSP has:

- executed;
- acquired; or
- in the case of a payment initiation service provider (PISP), initiated;

and that the PSP deems to fall into either of the following categories:

- 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
- 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').

If a payment transaction meets the conditions above it should be recorded as a fraudulent transaction for the purposes of this report irrespective of whether:

- the PSP had primary liability to the user; or
- the fraudulent transaction would be reported as such by another PSP in the same payment chain.

As a general rule, for all types of payment services, the payer's PSP has to report, except for direct debit transactions, which are reported by the payee's PSP. In addition, card payments are reported both by the payer's PSP (the issuer) and the payee's PSP (the acquirer).

Fraud committed by the payment service user (known as first party fraud) should not be reported.

The payment service provider should not report data on payment transactions that, however linked to any of the circumstances referred to in the definition of fraudulent transaction (EBA Guideline 1.1), have not been executed and have not resulted in a transfer of funds in accordance with the provisions in the *Payment Services Regulations*.

The category of 'payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order' covers a broader range of payment types than what is known in the UK as 'authorised push payment fraud'. The latter is restricted to credit transfers authorised by the payer to a fraudster.

Table 1 - structure of the return

In summary, REP017 requires the PSP to report the following fraud types, divided into sections for different payment and e-money services:

for credit transfers (including those initiated by PISP):

- issuance of a payment order by the fraudster;
- modification of a payment order by the fraudster;
- manipulation of the payer by the fraudster to issue a payment order;

for direct debits where consent is given via an electronic mandate or separately where consent is given in another form:

- unauthorised payment transactions;
- manipulation of the payer by the fraudster to consent to a direct debit;

debit card transactions and separately for credit card transactions:

- issuance of a payment order by a fraudster, broken down into:
  - lost or stolen card;
  - card not received;
  - counterfeit card;
  - card details theft;
  - other;
- modification of a payment order by the fraudster;
- manipulation of the payer to make a card payment;

cash withdrawals:

- issuance of a payment order by the fraudster refers to the following types of unauthorised card payment transactions, broken down into:
  - lost or stolen card;
  - card not received;
  - counterfeit card;
  - other; and
- manipulation of the payer to make a cash withdrawal.

for e-money transactions – to be reported by e-money issuers:

- issuance of a payment order by the fraudster;

- modification of a payment order by the fraudster;

- manipulation of the payer by the fraudster to issue a payment order;

for money remittance:

- fraudulent payment transactions.

Table 1 - fraud types

Below we provide guidance on the fraud types referred to in REP017. We give examples of these fraud types in relation to each payment or e-money service. PSPs should use their discretion when determining the appropriate fraud type for each fraudulent transaction and should choose the fraud type that most closely matches the circumstances of the fraud.

Credit transfers

Issuance of a payment order by the fraudster

This covers unauthorised payment transactions in which the fraudster uses stolen personalised security credentials in order to issue a payment order, either through contacting the victim's bank or accessing the victim's online banking service. For example, where a victim's online banking has been accessed using stolen personal identity details and credit transfers have been made from the victim's account to beneficiaries chosen by the fraudster.

Modification of a payment order by the fraudster

This covers unauthorised payment transactions where the fraudster has gained unauthorised access to the victim's account in order to change the details of existing payment orders or payment instructions. For example, where a victim's account has been accessed using stolen personalised security credentials in order to modify the beneficiary of the victim's existing standing orders. A victim's account could be accessed by a fraudster in order to modify a batch of payment details so that when payments are executed by the victim's PSP, the funds are unintentionally transferred to a beneficiary or beneficiaries chosen by the fraudster rather than the intended beneficiary. (See CIFAS paper, Table 2 Unlawful obtaining or disclosure of personal data: https://www2.cipd.co.uk/NR/rdonlyres/710B0AB0-ED44-4BD7-A527-B9AC29B28343/0/empfraud.pdf)

Manipulation of the payer by the fraudster to issue a payment order

This covers fraud where the payer authorises a push payment to an account the payer believes belongs to a legitimate payee, however, the payer was deceived into inputting the sort code and account number (or other unique identifier) of a fraudster, or an account controlled by a fraudster. This is also referred to as 'malicious misdirection'. For example, a scammer may contact a victim purporting to be from the victim's bank. The scammer may then convince the victim to transfer money (using a credit transfer) to a different account, purportedly in order to safeguard it. However, that account is in fact controlled by the scammer. (See Payment Systems Regulator response to Which? Super-complaint: https://www.psr.org.uk/psr-publications/news-announcements/which-super-complaint-our-response-Dec-2016).

Direct debits

Unauthorised payment transactions

This covers fraud where a victim's account details (e.g. sort code and account number) have been used by the fraudster to set up direct debit payments to an organisation, without the victim's knowledge or consent, resulting in unauthorised direct debit payments being taken from the account of the victim.

Manipulation of the payer by the fraudster to consent to a direct debit

This covers fraud where a payer is convinced by a fraudster to set up a direct debit and consent to payments being made to an intended payee (the legitimate payee), but the fraudster uses the victim's details and consent to set up direct debit payments to a different (unintended) payee.

Debit and credit cards:

Issuance of a payment order by a fraudster

Refers to the following types of unauthorised card payment transactions:

Lost or stolen card fraud

This covers any payment fraud committed as a result of a lost or stolen card (except where 'card not received fraud' has occurred). (See FFAUK Fraud Facts 2016 https://www.financialfraudaction.org.uk/fraudfacts16/assets/fraud_the_facts.pdf)

Card not received fraud

This covers fraud where a payment card is stolen (with or without the details of the PIN also being intercepted) whilst in transit – after the card company sends it out and before the genuine cardholder receives it. The payment card is then used by the fraudster to make transactions. (See FFAUK Fraud Facts 2016 https://www.financialfraudaction.org.uk/fraudfacts16/assets/fraud_the_facts.pdf)

Counterfeit card fraud

This covers fraud where the fraudster uses a card which has been printed, embossed or encoded so as to purport to be a legitimate card but which is not genuine because the issuer did not authorise the printing, embossing or encoding. (See https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/Fraud-the-Facts-A5-final.pdf)

Card details theft

This covers fraud where card details have been fraudulently obtained through methods such as unsolicited emails or telephone calls, digital attacks such as malware and data hacks, or card details being taken down from the physical card by a fraudster. The card details are then used to undertake fraudulent purchases over the internet, by phone or by mail order. It is also known as 'card-not-present' (CNP) fraud. (See https://www.financialfraudaction.org.uk/fraudfacts16/)

Other

Unauthorised transactions relating to other types of fraud should be recorded under 'other'.

Modification of a payment order by the fraudster (debit and credit card payments)

This is a type of unauthorised transaction 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 (e.g. payment card) 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.

Manipulation of the payer to make a card payment

This would cover card payments that have been authorised by the payer, i.e. using chip and pin, or authenticated online card payments. The customer believes they are paying a legitimate payee, i.e. a merchant, but the payee that receives the funds is not a merchant, but instead a fraudster.

Cash withdrawals

Issuance of a payment order by the fraudster

This refers to the following types of unauthorised cash withdrawals at ATMs, bank counters and through retailers ('cash back') using a card (or using a mobile app in place of a card):

- those resulting from a lost or stolen payment card;

- those resulting from a payment card being stolen (with or without the details of the PIN also being intercepted) whilst in transit – after the card company sends it out and before the genuine cardholder receives it; and

•those where the fraudster uses a card to withdraw money which has been printed, embossed or encoded so as to purport to be a legitimate card but which is not genuine because the issuer did not authorise the printing, embossing or encoding.

Manipulation of the payer to make a cash withdrawal

This refers to reported frauds where a payment service user has withdrawn under duress or through manipulation (using a card, or using a mobile app in place of a card).

E-money transactions

The same fraud types as above for debit and credit cards apply to payment transactions involving e-money.

Money remittance and payment initiation services

Fraudulent transactions

Money remitters and PISPs are required under the EBA Guidelines to report 'fraudulent transactions'. Money remitters and PISPs should use their discretion when determining what to count as a 'fraudulent transaction'. Where money remitters or PISPs detect the frauds described above, these should be counted as 'fraudulent transactions'.

Authentication method

For all credit transfers, card transactions and e-money transactions reported, including those initiated by PISP, the PSP should report whether strong customer authentication has been used or not. Strong customer authentication means authentication based on the use of two or more elements that are independent, in that the breach of one element does not compromise the reliability of any other element, and designed in such a way as to protect the confidentiality of the authentication data, with the elements falling into two or more of the following categories—

•something known only by the payment service user ("knowledge");

•something held only by the payment service user ("possession"); or

• something inherent to the payment service user ("inherence").

Where strong customer authentication is not used, the PSP should report under which of the following exemptions the transactions have taken place. These exemptions and their application are determined in the regulatory technical standards for strong customer authentication and common and secure open standards of communication (SCA-RTS). As noted in the FCA Approach Document, "The exemptions are separate and independent from one another. Where a payment transaction may qualify for an exemption under several different categories (e.g. a low-value transaction at an unattended card park terminal) the PSP may choose which, if any, relevant exemption to apply. PSPs should note that for the purpose of reporting fraud under regulation 109 of the PSRs 2017 and the EBA Guidelines on fraud reporting, fraudulent transactions should be assigned to a specific exemption and reported under one exemption only." (paragraph 20.39).

For the purposes of reporting, the applicable exclusions are:

•unattended terminal for transport or parking fares (article 12 SCA-RTS);

•trusted beneficiary (article 13 SCA-RTS);

•recurring transaction (article 14 SCA-RTS);

•low value (article 16 SCA-RTS);

•use of secure corporate payment processes or protocols (article 17 SCA-RTS);

•transaction Rik Analysis (article 18 SCA-RTS);

Data elements

Table 1 – Payment transactions and fraudulent payment transactions for payment services

Value should be reported in pounds sterling throughout (£)

Totals: Transaction and fraudulent transaction volume and value for all payment types

Guide to the relevant area of the form	PSPs should report the following information in respect of the payment type – e.g. credit transfers, direct debits etc:
2A-2L 38A–38L 48A–48L 103A–103L 155A–155L 167A–167L 199A–199L 200A–200L	•total domestic transaction volume (i.e. the number of transactions) for payment type – Column A; •total domestic transaction value for payment type Column B; •total transaction volume for payments made cross-border within the EEA – Column C; •total transaction value for payments made cross-border within the EEA – Column D; •total transaction volume for payments made cross-border outside the EEA – Column E; •total transaction value for payments made cross-border outside the EEA – Column F; •total domestic fraudulent transaction volume (i.e. the number of transactions) for payment type – Column G; •total domestic fraudulent transaction value for payment type Column H; •total fraudulent transaction volume for payments made cross-border within the EEA – Column I; •total fraudulent transaction value for payments made cross-border within the EEA – Column J; •total fraudulent transaction volume for payments made cross-border outside the EEA – Column K; and •total fraudulent transaction value for payments made cross-border outside the EEA – Column L. **PSPs should continue to report fraud data broken down into domestic, cross border within the EEA, and cross border outside the EEA as set out in Columns A-F, notwithstanding the UK's withdrawal from the EU.**

The above reporting pattern for columns A-L is repeated for all subsequent rows, except the following rows where only columns G to L are to be reported for the fraudulent transaction volume and value relating to the fraud type:

Credit transfers

8-10

12-14

23-25	
27-29	
Direct debits	
40-41	
43-44	
Card payment (except cards with an e-money function only)	
55-62	
64-71	
81-87	
89-95	
Card payment acquired (except cards with an e-money function only)	
110-117	
119-126	
134-140	
142-148	
Cash withdrawals	
158-163	
E-money payment transactions	
170-172	
174-176	
185-187	
189-191	
Initiated by payment initiation service providers	
3A-3L	Of the total transaction and total fraudulent transaction volumes and values for **credit transfers**, PSPs should report the volume and value of those initiated by payment initiation service providers.
Payment initiation channel – initiated non-electronically	
4A–4L (credit transfers) 49A–49L (card payments) 104A-104L (card payments acquired)	Of the total transaction and total fraudulent transaction volumes and values for **credit transfers** and **card payments only**, PSPs should report the volume and value of those initiated non-electronically. Transactions initiated non-electronically include payment transactions initiated and executed with modalities other than the use of electronic platforms or devices. This includes paper-based payment transactions, mail orders or telephone orders.
Payment initiation channel – initiated electronically	
5A–5L (credit transfers) 50A–50L (card payments) 105A–105L (card payment acquired)	Of the total transaction and total fraudulent transaction volumes and values for **credit transfers** and **card payments only**, PSPs should report the volume and value of those initiated electronically.
Remote transactions	

6A-6L (credit transfers) 51A–51L (card payments) 106A–106L (card payments acquired) 168A–168L (e-money payment transactions)	Of the total transaction and total fraudulent transaction volumes and values for **credit transfers**, **card payments** and **E-money payment transactions only** PSPs should report the volume and value of those that are remote transactions. A 'remote transaction' means a payment transaction initiated via the internet or through a device that can be used for distance communication (Regulation 2 of the *Payment Services Regulations*).
Non-remote transactions 21A–21L (credit transfers) 77A–77L (card payments) 130A–130L (card payments acquired) 183A–183L (e-money payment transactions)	Of the total transaction and total fraudulent transaction volumes and values for **credit transfers**, **card payments** and **E-money payment transactions only** PSPs should report the volume and value of those that are non-remote transactions. Non-remote means any payment transactions that are not initiated via the internet or through a device that can be used for distance communication.
Credit and debit card transactions **Card payments** 52A–52L (remote > debit) 53A–53L (remote > credit) 78A–78L (non-remote > debit) 79A-79L (non-remote > credit) **Card payments acquired** 107A–107L (remote > debit) 108A–108L (remote > credit) 131A–131L (non-remote > debit) 132A–132L (non-remote > credit)	For the total remote and total non-remote card transactions, PSPs should report the volumes and values that were credit card (including charge card) transactions and the volumes and values that were debit card transactions.
Strong customer authentication **Credit transfers** 7A–7L (remote > SCA) 11A–11L (remote > non-SCA) 22A–22L (non-remote > SCA) 26A–26L (non-remote > non-SCA) **Card payments** 54A–54L (remote > SCA) 63A–63L (remote > non-SCA) 80A–80L (non-remote > SCA) 88A–88L (non-remote > non-SCA) **Card payments acquired** 109A–109L (remote > SCA) 118A–118L (remote > non-SCA 133A–133L (non-remote > SCA) 141A–141L (non-remote > non-SCA)	For total remote and total non-remote credit transfers, card transactions, e-money payment transactions and payment transactions initiated by payment initiation service providers, PSPs should report the volumes and values of sent and fraudulent transactions authenticated via strong customer authentication and via non-strong customer authentication

E-money payment transactions	
169A–169L (remote > SCA)	
173A–173L (remote > non-SCA)	
184A–184L (non-remote > SCA)	
188A–188L (non-remote > non-SCA)	
Payment transactions initiated by payment initiation service providers	
202A–202L (remote > SCA)	
203A–203L (remote > non-SCA)	
205A–205L (non-remote > SCA)	
206A–206L (non-remote > non-SCA)	
Payment transactions initiated by payment initiation service providers	
207A–208L	Payment initiation providers reporting total transactions and total fraudulent transactions initiated, should report the value and volume of transactions that were credit transfers and the volume and value of other types of transactions that were using other payment instruments.
Fraud types	
Credit transfers	For remote transactions that were authenticated via strong customer authentication and non-strong customer authentication, PSPs should record the fraudulent transactions under the relevant fraud type (see guidance above).
8–10	
12–14	
23–25	
27–29	The same should be done for non-remote transactions.
Direct debits	
40–41	
43–44	
Card payment (except cards with an e-money function only)	
55–62	
64–71	
81–87	
89–95	
Card payment acquired (except cards with an e-money function only)	
110–117	
119–126	
134–140	
142–148	
Cash withdrawals	
158–163	
E-money payment transactions	
170–172	
174–176	

185–187	
189–191	
Fraudulent transactions broken down by exemption from SCA	
Credit transfers 15A–20L 30A–34L **Card payments** 72A–76L 96A–99L **Card payments acquired** 127A–129L 149A–151L **E-money payment transactions** 177A–182L 192A–195L	Of the transactions authenticated without strong customer authentication, PSPs should provide the fraudulent transaction volumes and values, broken down by which exemption was used as per guidance above.
Losses due to fraud per liability bearer	
35A, 36A, 37A, 45A, 46A, 47A, 100A, 101A,102A, 152A, 153A, 154A	PSPs are required to report the general value of losses borne by them and by the relevant payment service user, not net fraud figures. The figure that should be reported as 'losses borne' is understood as the residual loss that is finally registered in the PSP's books after any recovery of funds has taken place. The final fraud losses should be reported in the period when they are recorded in the payment service provider's books. We expect one single figure for any given period, unrelated to the payment transactions reported during that period. Since refunds by insurance agencies are not related to fraud prevention for the purposes of the *Payment Services Regulations*, the final fraud loss figures should not take into account such refunds.

Table 2 - Fraud relating to account information services		
Number of incidents of fraud		
209A	Please indicate the number of incidents of fraud	This should be the total number of incidents of fraud that the AISP has recorded. If there are no incidents of fraud, please enter '0' (there is no need to complete the rest of Table 2).
Total value of fraud across all incidents (or an estimation of the loss to the persons defrauded (£))		
209B	Total value of fraud	Where known, the AISP should report the value of any fraudulent transactions that were executed or initiated (by a third party PSP) as a result of the fraud committed against the AIS user or the AISP. In all other circumstances, the AISP should provide an estimation of the loss to the persons defrauded. In this Context, 'persons' includes the user of the AIS service, any other PSP (such as a credit institution that operated the payment account that the AISP accessed) or the AISP itself. 'Loss' includes loss of funds incurred as a result of fraudulent transactions and/or loss incurred as

		an indirect result of the fraud; for example, by having to reissue new payment instruments or fix breached security systems. If the fraudulent incident(s) did not result in any financial loss, the AISP should still report the incident, enter '0' at 214B and explain the type of fraud at 214C. AISPs should convert values for non-sterling transactions into sterling using the average ECB reference exchange rate for the applicable reporting period, where available. In other instances, AISPs should use the average of the applicable daily spot rate on the Bank of England's Statistical Interactive Database for the applicable reporting period.
Description of fraud		
209C	Description of fraud	AISPs should describe the type of fraud that has resulted in the highest total value of fraud in this section (unless the AISP is reporting fraudulent incidents that did not result in any financial losses, as above). AISPs should also explain how the losses were incurred (on the basis that the AISP did not come into possession of the payment transaction funds and was not responsible for the execution of payment transactions).