Fraud reporting under PSD2

FISER CONSULTING
FINANCIAL SERVICES

Contents

Fraud reporting under PSD2

In November 2015, the Payments Service Directive 2 (PSD2) was accepted as a regulative law. The Directive aims to protect consumers and companies when they conduct online payments, promote the development of innovative payment services with a higher customer experience, ensure technology and business-model neutrality; and integrate the payments markets in Europe.

In accordance with Article 96(6) in PSD2, a Payment Service Provider (PSP) must provide "statistical data on fraud relating to different means of payment to their competent authorities" and also states that the competent authorities, in turn, "will provide European Bank Authority (EBA) and the European Central Bank (ECB) with such data in an aggregated form".

The EBA released the Draft Guidelines (GL) on fraud reporting under PSD2 in August 2017. This document has the purpose of determining the details and rules that PSPs and Competent Authorities most follow to accurately report on fraudulent transactions that have occurred. A consultative process is underway whereby all related parties have provided their response. The final GL is expected to be released by November 2017 with enforcement on 13 January 2018 (NL requested an extension for PSD2 implementation to Spring 2018[1]). This is in line with existing Level 1 compliance deadlines.

A fraudulent transaction is defined as a condition where there is an unauthorised or fraudulent use or initiation of a payment service. The fraudulent transactions should be disclosed at the moment they are reported or discovered, rather than when the case was resolved.

The scope of the regulation includes PSP's and Competent Authorities but provides an exception on Account Information Service Providers (AISPs). This exception takes into account that fraud reporting is solely based on those transactions that had been initiated and executed (completed). Furthermore, the level of reporting depends on the payment service used. The regulation identifies as payment services: (1) e-money services, (2) money remittance services, (3) payment initiation services, (4) credit transfer, (5) direct debit services, (6) payment card issuance, and (7) payment card acquiring.

Generally, the fraud transaction reports will consider (a) Quantitative data, such as volume (number of fraud transactions) and value (monetary value of fraud transactions) at a specific period; (b) Qualitative characteristics such as geography, location of the fraud in the payment chain, authentication method, payment channel, and the means in which the fraudster gained access to the sensitive payment data are also required.

The reports also distinguish between gross and net transactions. The total gross fraudulent payment transactions refer to all the transactions occurred over a period. Moreover, the total net fraudulent payment transactions refer to the total of gross fraudulent payment transactions minus the number of fraudulent payment transactions that have been recovered. This distinction is important for EBA to evaluate the damage that the fraudulent transactions are causing to the system.

Once the regulation becomes applicable in 2018, PSP's will be required to submit a quarterly report and an annual report. The quarterly report will contain a higher level of information, in contrast with the annual report that is expected to provide a detailed level of data on the fraud transactions. Figure 1 shows the roadmap of the regulation and timings for the first series of reports.

[1] De Koning (2017) Implementation of PSD2 in the Netherlands delayed https://www.regulationtomorrow.com/the-netherlands/implementation-of-psd2-in-the-netherlands-delayed/

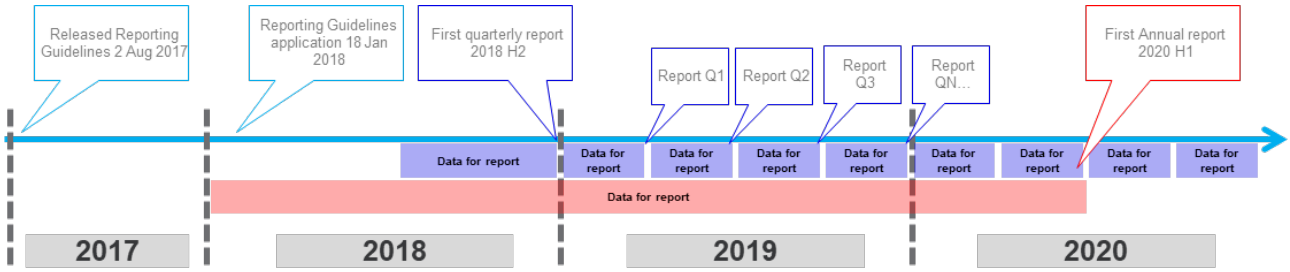

Figure 1.- Timeframes PSD2 fraud reporting

Reports per payment service

A PSP should recognise and correctly categorise the operated transactions in one of the EBA labels.

- Card Payments- A simple transaction where the cardholder makes a payment to a merchant or other entity by an electronic funds transfer.
- Credit Transfer. - Refers to the discount from one deposit account to another, it includes credit transfers performed via ATMs and transactions using cards with a credit or delayed debit function.
- Direct Debit- Denotes transactions that involve two parties i.e. the payee and the payer. The payee is the entity that directly receives the debit funds from the payer's account.
- E-money- Defined as an electronic mean, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for making payment transactions as defined e.g. companies that can be classified as e-money providers are PayPal and M-Pesa.
- Money remittance services- Refers to the services where an expatriate sends funds to their country of origin via wire, mail, or online transfer.

Each of the different transactions covered by PSD2 regulation will have a specific data requirement. Table 1 summarises the requirements for the quarterly and annual report. Each PSP should report accordingly with the requirements specified in GL Annexes 2 and 3.

Table 1.- Data requirements per transaction type

Payment service	Responsible reporting	Data breakdown summary	Reporting Periods
Card Payments	PSP payer and payee	Volume and value of all payment transaction and fraudulent transactions • Total transaction and fraudulent transactions • Payment channel • Authentication method • Reason for authentication choice • Fraud types • Transactions initiated via a PISP • Paper based and MOTO transactions (Annex 2, section D1)	Annual
		Volume and value transactions and fraudulent transactions Transactions initiated electronically • Total transactions and fraudulent transactions • Payment Channel • Authentication method • Transactions initiated by a PISP Payment transactions initiated electronically • Paper-based and MOTO transactions (Annex 3, section H1)	Quarterly
Credit Transfer	Payers PSP, because the payers initiate the transaction	Transactions Initiated Electronically • Total transactions and fraudulent transactions • Payment Channel • Authentication Method • Reason for authentication method • Fraud Type Transactions Initiated non-electronically • Paper based and MOTO Transactions (Annex 2, section D1)	Annual
		Volume and value transactions and fraudulent transactions. Transactions initiated electronically • Card function • Payment channel • Authentication method • Reason for authentication choice • Fraud types • Fraud subtypes • Transactions initiated by a PISP Transactions Initiated non-electronically • Paper based and MOTO Transactions (Annex 2, section D3)	Annual
	PSP of the payee's	Volume and value transactions and fraudulent transactions • Transactions initiated electronically • Total transactions and fraudulent transactions • Payment Channel • Authentication method • Reasons for authentication • Fraud types • Transactions initiated via a PISP (Annex 2, section D4)	Annual
Direct Debit	Payee PSP, (When the Payee initiate the transaction)	Volume and value of all payment transaction and fraudulent transactions • Total transactions and fraudulent transactions • Form of consent • Fraud Type (Annex 2, section D2)	Annual
		Volume and value of all payment transaction and fraudulent transactions • Total transactions and fraudulent transactions • Form of consent (Annex 3, section H2)	Quarterly

Payment service	Responsible reporting	Data breakdown summary	Reporting Periods
E-money	Payer's PSP, if the remittance and beneficiary are different. If the same the E-money provider	Volume and value of all payment transaction and fraudulent transactions • Total transactions and fraudulent transactions • Payment Channel • Authentication method • Reason for authentication choice • Fraud types (Annex 2, section A)	Annual
		Volumes and values of all payment transactions • Transactions and fraudulent transaction • Payment channel • Authentication method (Annex 3, section E)	Quarterly
Money remittance services	Payer's PSP not the PSP of beneficiary	Volume and value of all payment and fraudulent transactions • Total transactions and fraudulent transactions (Annex 2, section B)	Annual
		Volume and value of all payment and fraudulent transactions • Total transactions and fraudulent transactions (Annex 3, section F)	Quarterly
Transactions Initiated by PISP's	PSP	Volume and value of all payment and fraudulent transactions • Total transactions and fraudulent transactions • Payment instrument • Payment channel • Authentication method (Annex 2, section C)	Annual
		Volume and value of all payment and fraudulent transactions (net and gross) • Total transactions and fraudulent transactions • Payment channel • Authentication method (Annex 3, section G)	Quarterly
Card based payment transactions (Card was used in the sending side)	PSP was the payer's PSP	Volume and value of all payment and fraudulent transactions • Transactions initiated electronically • Card function • Payment channel • Authentication method • Authentication choice • Fraud types • Transactions initiated via PISP (Annex 2, section D3)	Annual
		Volume and value of all payment and fraudulent transactions • Transactions initiated electronically • Card function • Payment channel • Authentication method • Transactions initiated via a PISP • Transactions initiated non-electronically (Annex 3, section H3)	Quarterly
	PSP was the payee's PSP	Volume and value of all payment and fraudulent transactions • Total transactions and fraudulent transactions • Payment channels • Authentication method • Reason for authentication choice • Fraud types • Transactions initiated via a PISP • Transactions initiated non-electronically (Annex 2, section D4)	Annual
		Volume and value of all payment and fraudulent transactions Transactions initiated electronically • Total transactions and fraudulent transactions • Payment channel • Authentication Method • Transactions initiated by a PISP Transactions initiated non electronically • MOTO card based payment transactions (Annex 3, section H4)	Quarterly

Data management principles

Complying with the fraud reporting under PSD2 requires designing a Data Management Strategy and Reporting framework that adequately caters to the new requirements. A gap analysis should be considered in terms of determining if underlying systems which monitor fraud have the full set of required data to report. Timeframes for either enhancing existing systems or creating an additional data warehouse should be considered as soon as possible. Another important aspect is that the quality of the information should be traceable in case that the competent authorities need further information. Financial Institutions that are acting as PSP should consider the following features:

Cross-reference

Each fraud transaction detected and reported should be fully traceable inside PSP information systems. The EBA and ECB are looking at statistical patterns and correlations to consolidate the information provided, this will allow to detect fraudulent parties or control fragile entities in the Payment Value Chain.

Unique Category

A key component of the annual report is the categorisation of each of the transactions in their unique 'Fraud type'. The PSP should be capable of recognising and categorising the entire fraud transaction information in four types of buckets (1) Issuance of a payment order by the fraudster, (2) Modification of a payment order by the fraudster, (3) Manipulation of the payer to issue a payment order, (4) Payer acted fraudulently. Each fraud transaction can only be assigned to one category and overlapping should be avoided.

Each category must be mutually exclusive, and the total (volume or value) of payment transactions and fraudulent payment transactions should be the sum of each bucket. In the case of a series of payment transactions, or fraudulent payment transactions being performed, the PSP should consider each of those series of transactions as unique.

Duplicate registries

The GL recognises that the competent authorities would face the challenge of duplicate information at consolidation. This situation is not particularly an error because a fraud mechanism can affect different players in the payment chain. However, the GL dictates that is the responsibility of the entity that initiates the payment (payer or payee) to monitor and collect the required data.

Geography tracking

PSPs should be able to keep a close control of the transactions and fraudulent transactions that are performed in each of the countries that the institution operates. Based on that monitoring capability the PSP should differentiate transaction and fraud transactions in:

- Domestic (also refers as national). - Refers to transactions where the payer PSP and payee PSP are in the same EEA Member States.
- EEA cross-border payment transactions. - Denotes a transaction where the payers PSP and payee PSP are in different EEA Member States.
- Cross-border payment transactions 1 leg outside EEA. - Describes the transaction where 1 of the members involved in the transaction is outside an EEA member.

Time accuracy

PSP need to record on the day that the payment transactions and fraudulent payment transactions occurred for this statistical reporting. In the case of a series of transactions, the date recorded should be the date when each individual payment transaction was executed.

PSP should report all fraudulent payment transactions from the time fraud has been detected, such as through a customer complaint or other means, regardless of whether the case related to the fraudulent payment transaction has been closed by the time the data is reported.

Our Services and how we can help

FiSer Consulting can assist you in the transformation process of the following areas:

Business Consultancy, Requirement Engineering & Business Process Engineering

Due to our exclusive focus on Financial Services, our consultants have a strong content background which covers the Payments and Open Banking arena. A strong background and extensive knowledge of the organisation and processes, our consultants can assist you with:

- Interpretation and approach to the new European Banking Authority (EBA) Regulatory Technical Standards (RTS)
- Gap analysis, strategy definition and roadmap development
- Design of infrastructure and risk controls to support PSD2 and Open Banking
- Changes with operating models
- Assisting with developing an API plan and strategy which includes assistance with technology selection and implementation

Business Case Advisory

With a major change to your technology infrastructure as well as far reaching implications for the entire business, our consultants can formulate and develop a solid Business Case which will cover:

- A description of the business challenge
- An assessment of the potential benefits and costs of the PSD2 and Open Banking investment
- An assessment of the risks that may arise during the implementation/change program
- Recommendations on a preferred course of action
- Description of the implementation approach

Project & Program Management

The implementation of PSD2 and Open Banking covers changes that effect many stakeholders of the organisation. Significant changes in the way of dealing with customers and other market participants ask for investments supporting advanced IT infrastructure and innovative technology. Our Project & Program Management capability can help you structure and manage a variety of stakeholders across your business. Our project & program managers combine multiple years of experience with in-depth knowledge of the Payments industry.

Project Management Support

Aligned with our Project & Program Management capability, the PSD2 and Open Banking implementation requires detailed and frequent risk & issue, planning & dependency management as well as internal status reporting. Our Project Management Officers, with proven experience within the Financial Services industry, assist the organisation in these challenging activities.

Glossary of terms

Term	Definition
EEA	European Economic Area
GL	Draft Guidelines on fraud reporting under PSD2
EBA	European Banking Authority
MOTO	Mail Order/Telephone Order
PISP	Payment Initiation Service Providers
Payer	Person who makes the payment
Payee	Person who receives the payment

Next steps

For further information on PSD2 and where FiSer Consulting can assist you, please contact:

FiSer Consulting | Mischa Wesdorp

Mischa brings over 14 years of experience in the Global Financial Services Industry where he has been employed mostly by large international Dutch based banks. In his career Mischa acquired an all-round understanding of Risk, Lending and Payments. He is specialised in Operational Risk and Payments related projects.

Contact: m.wesdorp@fiser.consulting

FiSer Consulting | Paul Nielsen

Paul has over 15 years of financial and project management experience across retail banking, investment banking, asset management, IT and FMCG sectors. He has extensive consulting skills in Basel II, Solvency II and Sarbanes Oxley regulatory reporting. Paul also has a wide-ranging understanding of FATCA, CRS, IFRS9 and MIFID requirements and implementation.

Contact: p.nielsen@fiser.consulting

FiSer Consulting | Roberto Nieves

Roberto has over 6 years of experience as management consultant, leading and promoting innovation for top financial institutions. Roberto's consulting skills are mostly in transformation management, business strategy, and compliance implementation with a deep understanding of retail and wholesale banking.

Contact: r.nieves@fiser.consulting

FISER CONSULTING
FINANCIAL SERVICES

Barbara Strozzilaan 201
Tel.: +31 20 20678386
1083 HN Amsterdam
www.fiser.consulting
The Netherlands