

# Summary of the risk assessment on the payment service sector

24.8.2020 Public

1 (9)

## Content

1	Purpose and scope of application of the sector-specific risk assessment.....	2
2	Preparation of the risk assessment .....	3
3	Risk assessment and its justifications .....	5
3.1	Sector-specific risk assessment.....	5
3.2	Risk categories .....	6
3.2.1	Products and services.....	6
3.2.2	Geographical risk .....	7
3.2.3	Customers .....	7
3.2.4	Distribution channels.....	7
3.3	Management method categories .....	8
3.3.1	Risk-based approach .....	8
3.3.2	Organisation of activities .....	8
3.3.3	Customer due diligence .....	8
3.3.4	Monitoring .....	9
3.4	Money or Value Transfer Service Providers (MVTs providers).....	9

## Writer

❖ Viivi Jantunen / viivi.jantunen(at)finanssivalvonta.fi or tel. +358 9 183 5008

## 1 Purpose and scope of application of the sector-specific risk assessment

The sector-specific risk assessment on money laundering concerning payment services is an assessment by the Financial Supervisory Authority (FIN-FSA) on the sector-level risk of money laundering faced by entities under the notification obligation providing payment services. In contrast to the assessment of inherent risk, the sector-specific risk assessment takes into account factors pertaining to individual entities under the notification obligation, but the assessment has been prepared with a view to the sector as a whole. The assessment covers payment service providers referred to in the Payment Institutions Act (297/2010), and this risk assessment does not delve into payment services provided by credit institutions.

The scope of application of the Anti-Money Laundering Act (AML Act) includes the following payment service providers referred to in the Payment Institutions Act.

1. Authorised payment institutions referred to in section 6 of the Payment Institutions Act and Finland-based branches of foreign payment institutions
2. Payment service providers referred to in sections 7 and 7 a of the Payment Institutions Act, which provide services by virtue of registration
3. Foreign payment institutions providing services in Finland through an agent without establishing a branch.

This risk assessment concerns the following groups:

- **Payment institutions**, i.e. entities referred to above in paragraph 1
- **Registered payment service providers**, i.e. entities referred to above in paragraph 2, excluding entities providing money remittance referred to in section 1(2)(5) of the Payment Services Act (290/2010) as their only payment service.
- **Money or Value Transfer Service (MVTs) providers** i.e. entities providing money remittance referred to in section 1(2)(5) of the Act on Payment Institutions as their only payment service<sup>1</sup>.

Foreign payment institutions providing services in Finland through an agent without establishing a branch are not covered by this risk assessment, since they do not yet have reporting obligations in Finland at the time of the risk assessment.

The assessment takes into account payment services defined in section 1, subsection 2 of the Payment Services Act.

- 1) service for making a cash deposit on a payment account or withdrawing cash from a payment account and activities related to the operation and provision of a payment account;
- 2) execution of a payment transaction as a credit transfer, transfer of funds on a payment account of a service provider, direct debit or through a payment card or other payment device;
- 3) issuing of a payment instrument;
- 4) acceptance and processing of a payment transaction, based on a contract made with the payee, that results in a transfer of funds to the payee;
- 5) money or value transfers services (MVTs);
- 6) payment initiation service (PIS);
- 7) account information service (AIS).

A payment institution may be authorised to issue electronic money, and therefore the issuing of e-money has also been taken into account in the assessment of products and services. In addition to the

---

<sup>1</sup> Even though the service itself is called money remittance, in this document FIN-FSA refers to those providing money remittance services in Finland as MVTs providers as this is the term commonly used in e.g. Financial Action Task Force's publications.

abovementioned services, a payment service provider may provide currency exchange services, a switching service referred to in chapter 15 a of the Credit Institutions Act and other comparable operational services or additional services closely linked to payment services; and to maintain and provide payment systems. As regards other services than payment services that are allowed to payment service providers, currency exchange services are taken into account in the risk assessment. It is also considered whether the payment service provider has been registered as a virtual currency provider.<sup>2</sup>

## 2 Preparation of the risk assessment

In the assessment of money-laundering risks, the FIN-FSA applies the following four-step scale, which corresponds to the assessment scale used by the European Banking Authority. A corresponding risk score is defined to describe each risk level.

Risk level	Risk rating corresponding to the risk level
Very Significant	4
Significant	3
Moderately Significant	2
Less Significant	1

The sector-specific risk assessment consists of risk levels related to the risk and management method categories. In brief, the assessment of the risk level of the risk and management method categories was conducted as follows:

### 1) Risk category – products and services

In the assessment of risks related to products and services, the inherent risk levels determined for products and services in the FIN-FSA's assessment of inherent money-laundering risk<sup>3</sup> were utilised. As regards the products and services of the payment service sector<sup>4</sup>, it was scrutinised what kind of services are actually being provided in the sector and what kind of money laundering risk is involved in them.

The following aspects, among others, had a bearing on the risk assessment:

- What is the content of the services provided?
- How large is the group of entities providing the service concerned?
- What kind of special characteristics (risk-mitigating/accentuating features) are related to the services provided?

Sources:

- FIN-FSA and the Bank of Finland data collections:
  - RA – survey of risks and controls of money laundering and terrorist financing
  - MATI – survey of payment statistics
  - ML – survey of total payment transactions
- Information obtained at the authorisation and registration phase, in ongoing supervision and from the supervisors responsible for general supervision of payment service providers.

<sup>2</sup> Act on Virtual Currency Providers 572/2019.

<sup>3</sup> [https://www.finanssivalvonta.fi/contentassets/51ccf1c859b542df8a91dfc34bdd0d5b/julkaistava\\_fiva\\_ml\\_riskiarvio\\_en.pdf](https://www.finanssivalvonta.fi/contentassets/51ccf1c859b542df8a91dfc34bdd0d5b/julkaistava_fiva_ml_riskiarvio_en.pdf)

<sup>4</sup> Products and services referred to above in section 1 on the scope of the risk assessment.

## 2) Risk categories – geographical risk, customers and distribution channels

In addition to products and services, the risk assessment must also always consider risk factors related to customers, the geographical location and distribution channels. In order to assess these risk factors, the data reported on customers, distribution channels and the geographical dimension by payment service providers in the RA survey were reviewed. In addition, data collected on the geographical dimension of payment traffic in the MATI and ML surveys was utilised.

## 3) Management method categories

The RA survey is also used to collect data on risk management methods used by supervised entities. The data reported by supervised entities in the RA survey involves broad-based quality problems, since PSPs have not always reported the data in accordance with the reporting instructions. In preparing the sector-specific risk assessment, the section on management methods also draws upon information obtained in the authorisation and registration process, in ongoing supervision and from inspections, in addition to the RA survey.

## 3 Risk assessment and its justifications

### 3.1 Sector-specific risk assessment

The FIN-FSA has assessed that the risk of money laundering concerning the payment service sector as a whole is **significant**. Within the sector, the risk level concerning the various sub-groups was considered to be the following:

Group	Risk level
• Payment institutions	Moderately Significant
• Registered PSPs	Significant
• MVTSP's	Very Significant
<b>Payment service sector, total</b>	<b>Significant</b>

Sections 3.2 and 3.3 discuss the justifications of the risk assessment concerning payment institutions and registered PSPs. The justifications of the assessment concerning MVTSP providers are described in a separate section 3.4: *Money or Value Transfer Service providers*.

The risk levels determined for the various risk and management method categories are presented in the table below:

Risk categories:	Payment Institutions	Registered PSPs	MVTSP providers
• Products and services	Moderately Significant	Moderately Significant	Very Significant
• Geographical location and payment traffic	Moderately Significant	Moderately Significant	Very Significant
• Customers	Significant	Significant	Significant
• Distribution channels	Significant	Significant	Very Significant
<b>Risk level of risk categories:</b>	<b>Moderately Significant</b>	<b>Moderately Significant</b>	<b>Very Significant</b>
<b>Management method categories:</b>			
• Risk-based approach	Significant	Very Significant	Very Significant
• Organisation of activities	Less Significant	Significant	Significant
• Customer due diligence	Significant	Very Significant	Very Significant
• Monitoring	Significant	Very Significant	Very Significant
<b>Risk level of management method categories:</b>	<b>Significant</b>	<b>Very Significant</b>	<b>Very Significant</b>
<b>Overall risk level</b>	<b>Moderately Significant</b>	<b>Significant</b>	<b>Very Significant</b>

## 3.2 Risk categories

### 3.2.1 Products and services

The products and services provided have a crucial role underlying the risk of a sector or individual entity to be abused in money laundering. Therefore, the risk level of products and services was weighted in the assessment more than the other categories. As stated above, the products and services assessed included, in addition to payment services under the Payment Services Act, also currency exchange, virtual currency services and electronic money.

The inherent risk levels of products and services were determined in the summary of the supervisor-specific risk assessment of inherent risk published on 17 March 2020 by the FIN-FSA<sup>5</sup>. According to the FIN-FSA's assessment of inherent risk, the majority of products and services of the payment service sector were assigned either a *very significant* or *significant* risk rating. The reason is that the risk of money laundering is inherently high in products and services enabling the transfer of funds from one place or person to another.

The categorisation of products and services in the payment service sector were adjusted slightly from that used in the assessment of inherent risk based on information collected for the sector-specific risk assessment. The changes compared to the categorisation used in the assessment of inherent risk are the following:

- Payment accounts were combined with cash services.
- Payment services (excl. payment accounts and MVTs) are changed into Execution and acquiring of payment transactions.
- The issuing of e-money and other payment instruments comprise a single group of services.

Product/service-specific inherent level of risk
Payment Accounts (incl. cash services)
Execution and acquiring of payment transactions
Money or value transfer services (MVTs)
Virtual asset services
Currency exchange
E-money and issuing of payment instruments
Payment initiation service (PIS)
Account information service (AIS)

In determining the risk related to products and services at the sector level, a higher weight was assigned to products and services with a higher level of inherent risk. For example, payment account products (inherent risk level *very significant* /4) at the sector-specific risk level have a higher weight than account information services (*less significant* /1).

The majority of payment institutions and registered payment service providers provide services related to the execution and acquiring of payment transactions. These services involve a high level of inherent risk, and therefore the risk related to these services at the sector level is also high. Payment accounts are

<sup>5</sup> [https://www.finanssivalvonta.fi/contentassets/51ccf1c859b542df8a91dfc34bdd0d5b/julkaistava\\_fiva\\_ml\\_riskiarvio\\_en.pdf](https://www.finanssivalvonta.fi/contentassets/51ccf1c859b542df8a91dfc34bdd0d5b/julkaistava_fiva_ml_riskiarvio_en.pdf)

provided by relatively fewer PSPs, and payment accounts provided by PSPs involve risk-mitigating elements for example in comparison with deposit accounts provided by deposit banks.

Money or value transfer service is a high-risk payment service, but it is provided by very few payment institutions or registered PSPs. Only a single payment institution and a few registered providers are authorised to issue e-money, and only few PSPs have issued payment instruments. The FIN-FSA is not aware of how many PSPs provide currency exchange services, and therefore the assessment relies on the inherent risk level in this respect.

The provision of virtual currency services requires separate registration. One payment institution has been registered as a virtual currency provider. Only a payment institution may provide payment initiation services, and there are only three such service providers. The inherent risk of account information services is low, and there are only five service providers.

### 3.2.2 Geographical risk

In terms of geographical risk, on the one hand, the location of entities' establishments and provision of services in different geographical areas was taken into account, and on the other hand the geographical dimensions of payment traffic.

The assessment concerning location only concerns payment institutions, since registered PSPs do not have the possibility to provide services in other EU countries through a branch or an agent or directly across the border based on notification. Finnish payment institutions have relatively few branches, subsidiaries or agents outside Finland. This has an impact reducing geographical risk. A considerable amount of services provided directly across the border has been notified in the EEA, which in turn increases the geographical risk. However, geographical risk concerning the EEA is lower compared to circumstances where services were provided outside the EEA or in high-risk countries.

As regards payment traffic, it was found that a majority (80%) of payment transactions executed by both payment institutions and registered PSPs were domestic transactions. Furthermore, the majority of cross-border payment transactions were EU/EEA transactions.

### 3.2.3 Customers

Payment institutions and registered PSPs' level of risk was considered *significant*.

Data on customers was collected in the RA survey. The level of risk concerning customer depends on, among other things, the number of the entities' foreign customers, high-risk customers and customers in certain higher-risk sectors. Inconsistencies were identified in the data on customers reported by payment institutions and registered PSPs in the RA survey, which has an impact elevating the risk level.

### 3.2.4 Distribution channels

Payment institutions' and registered PSPs' level of risk concerning distribution channels was considered *significant*.

The assessment emphasises the fact that almost all service providers provide services through the online channel. The online channel has traditionally been considered to raise the risk level, since in this case business is conducted solely on remote basis.<sup>6</sup> Few have physical service points. Some entities

---

<sup>6</sup> DIRECTIVE (EU) 2015/849 (Fourth Anti-Money Laundering Directive), Annex III

have reported they also conduct business at a home address, but according to information obtained from senior financial supervisors responsible for them, they also have premises intended for the operation of the company.

### 3.3 Management method categories

In the assessment of management methods, the sector-specific risk assessment mainly draws on data reported by payment institutions and registered PSPs in the RA survey. Hence, the assessment is based on data reported by the entities themselves, and the validity of the responses has not been verified.

#### 3.3.1 Risk-based approach

For payment institutions, the risk level concerning the risk-based approach to activities was considered *significant* and for registered PSPs, it was found *very significant*.

As regards payment institutions, the primary factor elevating the risk is that the risk evaluation made on the customer is not taken into account in the ongoing monitoring of the customer relationship. As regards registered PSPs, the risk evaluations lack elements required by the law, and not all entities have procedures in place for the evaluation of risks pertaining to the customer.

#### 3.3.2 Organisation of activities

Payment institutions have mainly reported that they have the operating guidelines and procedures required by the ALM Act as well as training and practical work instructions to ensure compliance with customer due diligence procedures. Therefore, the risk level for the category was determined as *less significant*.

Meanwhile, registered PSPs had some outdated operating principles, procedures and practical work instructions. Therefore, their risk level was determined as *significant*.

#### 3.3.3 Customer due diligence

As regards customer due diligence, there were challenges particularly in the quality of the data collected in the RA survey. This concerns especially data related to the updating of customer information. For payment institutions, the risk was determined as *significant*, while for PSPs, it was found to be *very significant*.

The quality of data on payment institutions was higher, but nevertheless many of them reported that customer information had not been updated, even for high-risk customers. Many entities used third-party services or services of an outsourced provider to comply with customer due diligence obligations, which elevates the risk. Similarly, it plays a role that new methods such as video identification or another method undefined in the response alternatives are used in verifying the identity of the customer.

As regards registered PSPs, according to data on the updating of customer information, the majority of entities had not updated customer due diligence information at all in the past couple of years. Going forward, it remains to be examined to what extent the responses are explained by the fact that the requisite information is not available in the reporters' systems. Based on the responses, there are shortcomings in statutory procedures concerning the agent and beneficial owner. Furthermore, a considerable number of respondents stated they use a non-conventional method (passport, personal identification card, driver's licence or strong electronic authentication method) to verify the customer's identity.

## 3.3.4 Monitoring

As regards monitoring, the assessed risk level was *significant* for payment institutions and *Very significant* for registered PSPs.

Almost all payment institutions have a systems-based solution to monitor payment traffic. Monitoring generates quite different numbers of hits for different entities, whereof a relatively low number is notified to the Financial Intelligence Unit (FIU) of the National Bureau of Investigation. The low number of notifications to the FIU requires further investigation within the scope of ongoing supervision. It is also noteworthy that some of the payment institutions have not arranged enhanced monitoring for politically exposed persons as required by the law.

All registered PSPs indicated in the RA survey that they monitor payment traffic either by a systems-based solution or manually. However, monitoring generates a low number of hits leading to internal investigation, and it is alarming that only two entities reported they had filed a notification with the FIU. The majority also reported they had no statutory enhanced supervision in place for politically exposed persons.

## 3.4 Money or Value Transfer Service Providers (MVTs providers)

MVTs providers provide money remittance referred to in section 1, subsection 2, paragraph 5 of the Act on Payment Institutions as their only payment service. Money remittance means a service where the payment service provider takes receipt of funds from a customer in order to remit them to a payee designated by the customer without setting up a payment account for the payer or the payee. The funds may be remitted either directly to the payee or to another payment service provider acting on behalf of the payee. Money remittance also refers to a service where the service provider takes receipt of funds on behalf of a customer and makes them available to the customer.

All registered MVTs providers operating in Finland operate as part of the hawala system. Hawala is an international MVTs system mainly used in areas within the scope of the Islamic culture. The hawala system is used in remitting money in particular to areas where the availability of banking services is weak. Money is remitted through hawalas operating in Finland for example to Northern and North-Eastern Africa, Middle East and Western Asia.

The risk of money laundering related to MVTs is *very significant* considering, among other things, that the funds remitted are often received in cash. The geographical risk of MVTs providers operating in Finland is *very significant* because the money or value transfers are made to areas with weak supervision by authorities and potentially significant shortcomings in AML/CFT procedures.

In connection with the review of the management methods in place, shortcomings were identified in the risk-based approach. Furthermore, it has been found in the context of supervision that the procedures applied in practice are not consistent with the operating instructions prepared for the activity concerned. Shortcomings have also been detected in the monitoring of customers and their transactions, in addition to which MVTs providers make considerably few notifications to the FIU on suspicious transactions.

The risk of money laundering pertaining to MVTs was assessed to be *very significant*.