FI Supervision

Observations from money laundering reporting

No 23

18 juni 2021

Ref. 21-4810

Contents

FI Supervision

Finansinspektionen publishes regular supervision reports in a numbered report series. These supervision reports are part of FI's communication. They describe investigations and other supervision carried out by FI. These reports enable FI to present its observations and assessments as well as its expectations in various matters. This information can support companies in their operations.

Finansinspektionen
SE-Box 7821, 103 97 Stockholm, Sweden
Street address Brunnsgatan 3
Telephone +46 8 408 980 00
Email finansinspektionen@fi.se
www.fi.se

Summary

Finansinspektionen (FI) has been expanding its supervisory work and this includes analysing and comparing the information that companies have reported to the authority between 2018 and 2021 as part of its money laundering supervision.[1] Analysing this reported data plays an important role in FI's risk-based supervision and is used as part of its risk identification and risk classification of companies. This analysis highlights areas where companies need to develop their processes to make them better able to manage the risk of being used for money laundering or terrorist financing.

Reported data used in the supervision

The Money Laundering Regulations aim to prevent financial operations being used by criminals for money laundering and terrorist financing. Companies that are supervised by FI and subject to the Money Laundering Regulations submit information annually about their operations and the measures they take to comply with the Money Laundering Regulations. FI then compiles and assesses this data so that it can develop an understanding of the risks involved in the various financial sectors and, ultimately, assess the risks of every company. This risk assessment is used when planning future supervisory measures. However, the aim of this reporting process is not to identify any violations of the regulations; the analysis is used to help set priorities for FI in its supervision for 2021. If FI is going to perform effective, risk-based supervision, it is important for the companies to report their data on time. We have now analysed the information reported in 2018–2021, which refers to the 2017–2020 financial years. The analysis has been performed at both company and sector level. FI presents a selection of the results from the analysis in this report.

Despite some improvements, there are still areas that continue to need attention

Although the proportion of companies that reported on time increased during the first three reporting years, there was a slight decrease for the year 2020.[2] It is also the case that some companies still do not submit their report on time or do not submit it at all. In these cases, FI is able to order the companies to fulfil their

[1] *FI:s arbete mot penningtvätt och finansiering av terrorism*, 15 November 2019. An English translation is available at www.fi.se.
[2] The deadline for reporting data for the year 2019 was extended by one month due to COVID-19. No similar allowances were granted for reporting data for the year 2020.

obligations and it is authorised to issue them with a fine. In terms of the reporting for the year 2019, FI issued 31 orders for failure to report and each incurred a fine.

The analysis of the reported data highlights the areas where companies must improve their work, according to FI. For example, many of the reporting companies have stated in all reporting periods that they have not had adequate and up-to-date customer data for all customers. Although there has been an improvement since 2017, companies must continually work to obtain adequate and up-to-date customer due diligence data.

Potential weaknesses were also found in relation to the general risk assessment. A general risk assessment is required by the regulatory framework, and it is one of the most central parts of combating money laundering and terrorist financing. This is why FI focuses on this area in its supervisory activities.

Another area where the periodic reporting has revealed potential weaknesses is the companies' assessment of which customers present a higher risk of money laundering; companies need to continue to make improvements in this area. These could be customers who are politically exposed persons or customers that are largely domiciled outside the EU/EEA.

The Money Laundering Act also requires companies to use a system for monitoring suspicious transactions. The reported data shows that some companies do not have this kind of system in place. FI has also seen significant variation in the effectiveness of the systems for monitoring and reporting suspicious transactions or behaviour to the Swedish Police Authority. This primarily relates to the management of the alarms generated by the monitoring systems and the subsequent reporting to the Swedish Police Authority. We have also noted that companies that conduct operations that typically involve a higher risk of being used for money laundering and terrorist financing have reported a relatively low number of suspicious transactions or activities to the Swedish Police Authority. These companies and their monitoring and reporting processes are a recurrent feature of FI's supervisory activities.

Periodic money laundering reporting

The periodic money laundering reporting is one of the tools used by Finansinspektionen's (FI) to assign a risk classification to the companies that FI is responsible for supervising. Risk classification plays an important role in FI's risk-based supervision and is used, inter alia, for planning the authority's supervisory activities.

The purpose of this reporting

Since 2018 companies that are subject to FI's money laundering supervision have to annually submit information to FI that the authority assesses as being essential to evaluate the risk of a company being used for money laundering or terrorist financing.[3] This data must be received by 31 March each year and relates to the companies' conditions for the preceding calendar year. There are approximately 2,000 operators who are subject to FI's money laundering supervision and most of them are obliged to submit information in this way; they range from major banks to individual insurance intermediaries and are referred to as 'reporting companies'.[4]

The aim of this reporting is not to identify violations of the regulations, but to assist in the risk identification work and the risk-based supervision. The reporting is based on a questionnaire that currently contains approximately 90 questions and is divided into the following sections.[5]

- Information about the company's operations
- The company's risk assessment and procedures
- Customer due diligence
- Monitoring and reporting
- Compliance
- Training

The report 'FI's work to combat money laundering and the financing of terrorism' states that an effective working method for identifying and classifying money

[3] See Chapter 7 of Finansinspektionen's regulations regarding measures against money laundering and terrorist financing (FFFS 2017: 11) (the Money Laundering Regulations), which entered into force on 1 August 2017.
[4] Not all companies are required to report this data ('non-reporting companies'). For example, some agents are excluded as well as branches that do not have a permanent establishment in Sweden.
[5] This is a self-assessment form for the reporting companies. The reported data has not been validated by FI. The questionnaire can be downloaded from www.fi.se.

laundering risks in financial companies that are subject to supervision plays an essential role in risk-based supervision.[6] When the reporting requirement was introduced, FI developed a method for effectively analysing and processing the reported data as part of its work to increase the capacity and quality of its money laundering supervision. This method compiles and assesses the information from the companies using a number of specific parameters. We further developed this method in 2020, inter alia, by assessing sector-specific risks, based on the experiences that we had gained from our supervisory activities. The method results in an individual risk classification for each operator. Not only does this information provide FI with an overview of threats and vulnerabilities in the financial sector, we also use the individual assessment directly in our supervision work, as it is a useful tool for prioritising investigations and other supervisory activities.

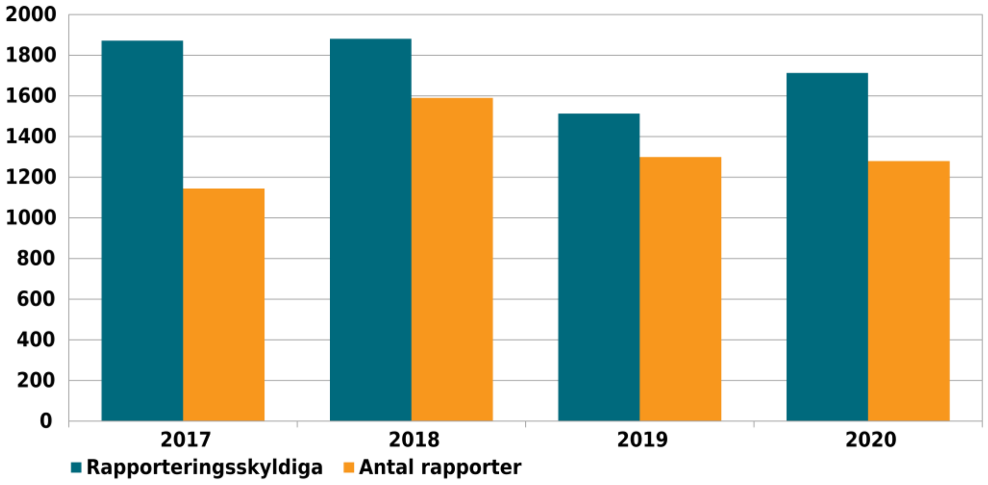
The periodic money laundering reporting is therefore important as it enables FI to carry out its assignment and to perform risk-based and appropriate supervision. This is why it is essential for reporting companies to report their data on time every year.

Late reports or no reports

FI has received reports from an average of approximately 80% of the reporting companies before the deadline. Since the introduction of the reporting obligation, the authority has seen an increase in the proportion of reports received on time. We work actively to ensure that companies comply with the reporting requirement, inter alia, by contacting companies that have been granted registration or authorisation, and by sending targeted reminders. If companies do not submit their reports, despite being sent reminders, FI is able to order these companies to report and it is also authorised to issue them with a fine. FI ordered 31 companies to submit their reports for the year 2019 as a result of their reports being late. A fine was issued for all of them.

[6] *FI:s arbete mot penningtvätt och finansiering av terrorism, 15 November 2019, page 21.* An English translation is available at www.fi.se.

1. Reports received over time



Source: FI

Note: The number reported on time relates to reports that were received before the final deadline for each year. Certain companies were excluded from the reporting obligation for the year 2019, which is why the number of reporting companies was lower for that year.

The national risk assessment for 2020 presents the results of a sector-by-sector risk analysis, where FI, along with 15 other authorities and the Swedish Bar Association, assessed the threats and vulnerabilities of the sectors subject to the Money Laundering Regulations.[7] The risk assessment presents evaluations of the threats and vulnerabilities that have been assessed for each sector. Banks and financial institutions account for the highest combined risk for the sectors subject to FI's supervision.[8] The proportion of companies that report on time for these sectors differs. Although banks consistently report on time, financial institutions do not, with a few financial institutions not submitting any reports at all. Reporting provides essential data for risk-based supervision, so it is especially important for the sectors that are particularly high-risk to report the data about their operations to FI.

Analysis of reported data

In this report we present our observations that relate to some of the central elements of the Money Laundering Regulations, as each of them are important cornerstones for an effective system for combating money laundering and terrorist financing.

[7] National Risk Assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021.

[8] A.a. p. 28.

The report presents a number of observations that highlight weaknesses and areas of improvement in the companies' work to combat money laundering and terrorist financing for the companies that are supervised by FI. These observations are based on the reported data from the last four years.

Limitations and definitions in this report

This report presents a number of diagrams and tables at an aggregated level. Unless otherwise stated in the individual diagram or table, categories of operators with fewer than five companies have been removed from the tables in order to protect confidentiality.

In this report *private customers* refer to the natural persons who are customers of an operator and *corporate customers* for legal entities that are customers of an operator. *Company* is also used consistently for operators, irrespective of whether the operations are conducted through a natural person or legal entity.

At the time this report was completed, not all companies had submitted data for the 2020 reporting period. We have taken this into consideration when analysing the data for this report.

General risk assessment

Companies that do not have an effective general risk assessment are at greater risk than other companies of being used for money laundering or terrorist financing. This risk assessment must be evaluated annually and updated when necessary. This is a particular focus area for FI in its supervision and the reported data shows that some companies need to make improvements.

Introduction

The general risk assessment is a central and fundamental part of a company's work to prevent money laundering and terrorist financing and it is also an absolute requirement in the regulations. If companies do not have an adequate general risk assessment, there is a risk that the procedures and guidelines that they use in their day-to-day operations will not be enough to manage the risks to which their operations are exposed. In this section, FI presents its observations about general risk assessments from the periodic reporting.

As part of the periodic reporting, companies must answer a number of questions about producing their general risk assessment as well as the procedures and guidelines that companies have in place for keeping this risk assessment up-to-date. The questions also ask about the countries that the companies are exposed to and which of these countries the companies consider to be high risk.

Fact box – The general risk assessment

An operator must produce a general risk assessment in accordance with Chapter 2 Section 1 of the Money Laundering and Terrorist Financing (Prevention) Act (2017: 630) (the Money Laundering Act). The purpose of this general risk assessment is to chart the risks of money laundering and terrorist financing to which the company may be exposed. This general risk assessment has to take into consideration the products and services that are supplied, the customers and the distribution channels, and any geographical risk factors. The company must also take into account any experiences that the company has had when reporting to the Financial Intelligence Unit of the Swedish Police Authority.

The general risk assessment has to be designed based on the size and nature of the company. In accordance with Chapter 2 Section 1 of Finansinspektionen's regulations regarding measures against money laundering and terrorist financing (2017:11) (the Money Laundering Regulations), this risk assessment must be evaluated at least once a year and updated whenever necessary, for example, if there are any major changes to the company's range of products and services.

As part of this general risk assessment, an operator must take into account the geographical risk factors in its operations, including where in the world the company's customers are established. An operator must also check whether its customers are established in a country referred to by the EU Commission as a 'high-risk third country'.[9] If this is the case, the operator must apply enhanced due diligence measures for this customer.[10]

Observations

The reported data shows that most companies updated their general risk assessment every year. Some companies stated that they had not updated it within the past year. Across the four reporting years, a small proportion of operators also stated that they had not updated their general risk assessment over the past year, many of whom stated that it was longer ago than this.

As part of the general risk assessment, a company must take into account the geographical risks associated with its operations. This means, for example, that the company must take into consideration where its customers are established and any risks that this could present to the company. FI has noted that almost half of the reporting companies have stated that they do not consider themselves to be exposed to any high-risk countries.

Conclusions

If the general risk assessment is to reflect the risks to which the company is exposed, it must also be updated when the company's conditions change. Companies must therefore evaluate their general risk assessment regularly and at least once a year. However, the reported data shows that not all companies have updated their risk assessment over the past 12 months. The fact that the general risk assessment has not been updated does not, by itself, necessarily mean that there are any weaknesses in a company's work to prevent money laundering, as the conditions for the company's operations may not have changed since the most recent update. On the other hand, because the world is constantly changing, there is a risk that this general risk assessment will not be as up-to-date; if the period of time between the updates is too long, the assessment might not be fully adapted to the operations and the risks that the company is currently exposed to.

The fact that a company has not identified any high-risk countries in its general risk assessment does not in itself mean that there are any flaws in its design. However, FI has identified a risk due to the fact that the high proportion of companies that have not identified any high-risk countries could partly be due to companies only

[9] In accordance with Chapter 3 Section 11 of the Money Laundering Act.
[10] In accordance with Chapter 3 Section 17 of the Money Laundering Act.

taking into consideration the countries where they are established, and have therefore not sufficiently taken into account where their customers are established. If a company has not identified any high-risk countries, the company should also be aware of any changes to its operations that could alter its geographical risk.

As the general risk assessment is such an important part of the company's preventive work, several of FI's recent investigations have included an audit of the companies' general risk assessment. These audits will continue in 2021.

Customer due diligence

Good customer due diligence plays an important role in an effective system for combating money laundering and terrorist financing. The reported data for money laundering enables FI to identify any inadequacies in the companies' data on business relationships and in the identification of high-risk customers. FI has also noted that these inadequacies differ between the various sectors.

Introduction

Adequate and up-to-date data about a company's customers is essential to understand and assess the risk of an individual customer. Any inadequacies in customer due diligence data can, for example, make it difficult for the company to detect any atypical behaviour from the customer or determine when it needs to apply enhanced customer due diligence measures. If a company does not have adequate knowledge of a customer, it cannot establish or maintain a commercial relationship or perform individual transactions.

The periodic reporting provides FI with data about the number of business relationships the companies have established in Sweden, the number of customers divided by their tax residency, and the number of the companies' established business relationships where customer due diligence data is not adequate nor up-to-date. The reporting also includes questions about the number of customers that the company has identified as being politically exposed persons or that are assessed as being high risk. In this section, we report on a selection of FI's observations of the companies' reported data on customer due diligence and the conclusions that can be drawn from this.

Fact box – Customer due diligence measures

The Money Laundering Act states that an operator may not establish or maintain a business relationship or carry out an individual transaction if the operator does not have adequate knowledge of the customer to be able to manage the risk of money laundering or terrorist financing that can be associated with the customer relationship. The operator must also have carried out adequate customer due diligence to be able to monitor and assess the customer's activities and transactions. The situations that require customer due diligence and the measures that need to be taken are primarily set out in Chapter 3 of the Money Laundering Act and Chapter 3 of the Money Laundering Regulations. For example, Chapter 3 Section 19 stipulates that a company must take enhanced customer due diligence measures for a politically exposed person (PEP). In accordance with Chapter 1

Section 8 Point 5 of the Money Laundering Act, a PEP is “a natural person who has or has had either an important public function in a state or a function in an international organisation”.

Established business relationships and inadequate customer due diligence

Observations

Between 2018 and 2020 companies have stated that the total number of established business relationships with Swedish customers amounted to just over 65 million. The ‘banking’ sector has by far the largest number of business relationships, at around four times higher than the ‘life insurance businesses’ sector. These two sectors combined account for approximately 85% of the number of business relationships. The banking sector’s proportion of the total number of business relationships in the financial sector has remained relatively stable during the four reporting years, at approximately 68%. The total number of business relationships for all companies has increased by approximately 7% since 2017. The payment service companies account for most of this increase, with the number of reported business relationships for the year 2020 approximately three times higher than in 2017.

Tabell 1. The number of reported business relationships in various sectors

Sector	Number of reporting companies as at 31 December 2019	Number of business relationships in 2019	Median number of business relationships in 2019
Banking or financing businesses	154	44,897,000	26,400
Life insurance businesses	44	11,513,000	87,200
Payment service providers	102	3,232,000	1,200
Fund operations	38	1,548,000	200
Consumer credit companies	79	1,275,000	1,400
Life insurance brokers	308	891,000	300
Other financial operations	346	786,000	100
Securities businesses	136	497,000	100
Housing credit companies	17	405,000	0

AIF managers	222	76,000	100
Total	1,449	65,120,000	200

Source: FI
Note: The data shown is for 2019 as there was insufficient data for 2020 at the time the report was being completed.

‘Housing credit companies’ are part of a relatively new sector that was added in 2016. This sector accounts for more than 400,000 business relationships, the majority of which relate to a few mortgage brokers, while relatively new companies that offer their own loans normally state that they have no or only a few customers; this explains why this sector’s median value for the number of business relationships per company is zero.

At the end of 2020, many of the companies assessed their customer due diligence as being inadequate for some of their customers. However, the analysis shows that the standard increased slightly in 2019 compared to 2017 and that this positive trend appears to have strengthened in 2020.[11]

The inadequacies in customer due diligence vary between sectors and over time. Companies in the banking sector reported that the proportion of inadequate data for private customers and corporate customers remained relatively stable between 2017 and 2019. For the year 2020, the reported data shows that the banks’ proportion of inadequate customer due diligence decreased overall, particularly for corporate customers. The proportion of inadequate customer due diligence in both customer categories also decreased between 2017 and 2020 for payment service providers, life insurance businesses, other financial operations and AIF managers. Companies involved in fund operations and life insurance brokers reported an improvement in terms of their corporate customers, but not for their private customers during this period. Securities businesses is the only sector that reported a slight increase in the proportion of inadequate customer records for both private customers and corporate customers as a whole between 2017 and 2020.

In terms of the various sectors, the consumer credit companies and housing credit companies stand out in a positive way, as they have consistently reported over the four years that their customer due diligence data was only inadequate for a negligible proportion of their entire sector.

Companies have to answer questions about whether they have any of the control functions mentioned in the Money Laundering Act.[12] An independent audit

[11] Based on data from the companies that were able to submit their data for the year 2020 by the time this report was completed.
[12] A specially appointed executive, central function manager and independent audit function pursuant to Chapter 6 Section 2 of the Money Laundering Act.

function is required in accordance with the Money Laundering Regulations, when this is justified based on the size and nature of the operations. One observation from the reported data for the year 2019 is that the companies that reported that they had an independent audit function also reported that they did not have customer due diligence data for a higher proportion of both private customers and corporate customers.[13] At the same time, we have noted that it is normally small companies that have reported that they do not have this kind of function.

Conclusions

As with the conclusions on the companies' work on the general risk assessment, there is more work that companies should be doing on their customer due diligence records. It is crucial for companies to have good knowledge of their customers, if they are to work effectively to combat money laundering and terrorist financing.

The reporting for the year 2019 shows that companies with an independent audit function have generally reported that they mostly do not have adequate customer due diligence data compared with companies that have stated that they do not have this function. FI believes that there is a risk for companies that do not have an independent audit function, regardless of the sector in which they operate, as they are less likely to have sufficient organisational conditions in place to determine which customer due diligence data is required to manage the risk of an individual customer and to ensure that they collect this data.

The stricter regulatory requirements in recent years and the increase in knowledge of the regulations, combined with new system support and internal processes, may be among the factors that, when combined, can lead to more internal requirements for determining the levels of customer due diligence data that is needed. Despite this, the number and proportion of customer records that companies consider to be inadequate decreased slightly between 2017 and 2020. This could indicate that companies are making more efforts in their customer due diligence measures.

Although the reported inadequacies have fallen over time, the reported data shows FI that there is a need for improvements. FI expects companies to work continuously to address any inadequacies and FI's risk-based supervision will continue to focus on this.

Politically exposed persons

Observations

A company that has customers who are politically exposed persons (PEP) must take certain enhanced due diligence measures for these customers. One of the

[13] An independent audit function has to be set up if this is justified based on the size and nature of the operations; see Chapter 6 Section 2 Point 3 of the Money Laundering Act.

questions that FI asks in the periodic reporting is the number of PEP customers that a company has.

The proportion of PEP customers in relation to the number of business relationships per sector varies between 25 and 275 PEPs per 100,000 business relationships. In the various sectors, the proportion of PEP customers varies greatly between the various companies. For example, the most recent reporting shows that the spread in the proportion of PEP customers is relatively evenly divided between 0 and 325 customers per 100,000 business relationships for companies with more than 100,000 customers in the life insurance businesses sector.

Tabell 2. Proportion of business relationships with a politically exposed person, broken down by sector

Proportion of PEPs per 100,000 business relationships

Sector	Proportion
Fund operations	275
AIF managers	162
Other financial operations	104
Life insurance businesses	84
Securities businesses	65
Banking or financing businesses	61
Consumer credit companies	57
Payment service providers	46
Housing credit companies	45
Life insurance brokers	25
Total, Proportion of PEPs per 100,000 customers	66

Source: FI
Note: These figures refer to the year 2020.

Conclusions

One reason for the large variation in the proportion of PEP customers between companies in the same sector could be the differences in the products and services provided by the companies and the customer segments targeted by the companies. However, there is a risk that some of these differences could also be due to the ability of individual companies to identify and manage this kind of customer. FI would therefore like to stress the importance of companies making sure that they have an appropriate and effective process in place for identifying PEP customers, so that the enhanced measures set out in the Money Laundering Act are always taken.[14]

Risk classification

Observations

In the periodic reporting, FI collects data on the proportion of customers that each company assesses as being high risk. The total average for all sectors is just under 1%, a figure that has remained stable over the past two years. Companies that conduct other financial operations[15] or consumer credit companies have reported that the proportion of high-risk customers was much higher overall for the year 2020. This difference can mostly be explained by a small number of companies that reported a relatively large number of high-risk customers. Housing credit companies are at the other end of the scale with only 1/20th of the average.

One observation from the periodic reporting for the year 2019 was that a number of companies that had stated that they did not have adequate and up-to-date customer due diligence data for a high proportion of their customers also reported that they only had a few high-risk customers or none at all. Although an improvement can be seen in this for the 2020 data, there were still several companies that had a high number of established business relationships that stated that they only had a few or no high-risk customers. It is also not unusual for the number of reported high-risk customers to be the same as the number of reported PEP customers. FI has also noted some ambiguities in the reporting from companies that have identified a number of customers as politically exposed persons, but have also reported that they do not have any high-risk customers; payment service providers, consumer credit companies and life insurance businesses are overrepresented in this respect.

Another factor that can indicate that a customer should be considered to be high risk, when combined with other factors, is if they have a tax residency outside the EU/EEA. The companies’ proportion of these customers is just under 1%, while the proportion is relatively evenly distributed between the various sectors. The only major discrepancy is in the companies registered in the ‘AIF-managers’ sector, where the average proportion is approximately three times higher than the other sectors. However, their average is significantly increased by a small number of companies that have a high proportion of customers in this category.

Conclusions

Having sufficient knowledge of a customer is a basic requirement to be able to understand and manage the risks involved in the customer relationship and to

[14] Chapter 3 Section 19 Points 1–3 Money Laundering Act.
[15] In accordance with the definition set out in Section 2 of the Certain Financial Operations (Reporting Duty) Act (1996:1006).

assign the correct risk class to the customer. The fact that some companies stated that they did not have adequate customer due diligence data for a high number of customers for the year 2019, while also reporting that they had almost no high-risk customers, raises questions. For the year 2020, the reported data shows that some of the companies that reported that they had customers who had been identified as politically exposed persons also reported that they only had a few high-risk customers, and, in some cases, none at all. FI would therefore like to stress how important it is for operators to ensure that they have an appropriate and effective process in place for the risk classification of their customers. The companies' risk classification of customers is therefore one of several parameters that FI uses in its risk-based prioritisation of supervisory activities.

Monitoring and reporting

Monitoring and reporting suspicious transactions is an important tool for combating suspected money laundering and terrorist financing. FI has noted significant differences in the way that companies monitor ongoing business relationships and transactions. There are also significant differences in the reporting of suspicious transactions to the Financial Intelligence Unit of the Swedish Police Authority, both for suspected money laundering and suspected terrorist financing.

Monitoring transactions

Introduction

Effective and appropriate systems and procedures for monitoring and reporting are essential for detecting and combating money laundering and terrorist financing. In this section, FI presents its observations of the companies' systems for monitoring customer transactions and activities.

Fact box – Monitoring transactions

In accordance with Chapter 4 Sections 1–3 of the Money Laundering Act, operators must monitor the transactions that are carried out in their operations. The reason for this is to detect transfers that deviate from what the operator has cause to expect, based on the knowledge it has of the customer, or what the operator has cause to assume, based on what it knows of its customers in general.[16] Another reason for monitoring transactions is to detect transfers that can be assumed to be connected to money laundering or terrorist financing, even if they do not deviate from what the operator has cause to expect. If these transactions are detected, the operator must investigate whether there are any reasonable grounds to suspect that money laundering or terrorist financing is involved. If an operator conducts an investigation and concludes that it has reasonable grounds to suspect money laundering or terrorist financing, it must report this to the Financial Intelligence Unit of the Swedish Police Authority without delay. As a general rule, the operator is also required to stop any suspicious transactions.

Monitoring transactions must be based on the customer due diligence that the operator carries out about the customer and the risk class that the operator has assigned the customer.

[16] Chapter 4 Section 1 of the Money Laundering Act

If an operator chooses to use an automated system based on models, the company must also apply a validation process that ensures that the model is fit for purpose.[17] The minimum requirement is for validation to be carried out when the model is launched and when there are any major updates to the model.[18]

Observations

A company must have some form of process in place to monitor its transactions. This process is called the *monitoring system* in this report, which is the same term used on the reporting form. This system can either be automated or manual. The regulations state that this monitoring must be risk-based and appropriate. For large companies, it is not practically possible to only use a manual monitoring system.

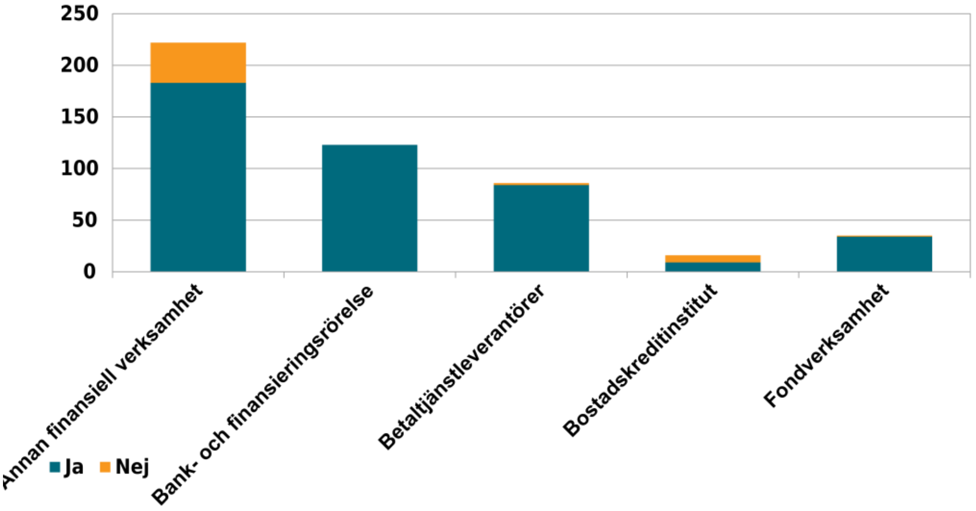
The companies that account for the majority of the total turnover and the number of business relationships in Sweden have reported that they have an automated monitoring system.[19] The proportion of companies with this kind of system has remained relatively stable over the three years that FI has obtained periodic money laundering reports. There are differences in the companies' transaction monitoring systems, as companies in some sectors are more likely than others to say that they do not have any kind of monitoring system (see Diagrams 2 and 3 below). The distribution of the sectors that do not have these monitoring systems, based on the reported data, has remained relatively constant over the four reporting years.

In their reporting, companies have to enter the length of time it takes from an alarm being generated in their monitoring system to the time when a suspicious activity report is submitted to the Financial Intelligence Unit of the Swedish Police Authority. FI reports that the median value for the time this takes differs between the various sectors. There are also differences between the companies in the various sectors.

[17] Models refer to procedures that aim to standardise and automate assessments that an operator has to carry out in order to meet the requirements set out in the Money Laundering Act, see Government Bill 2016/17:173 p. 547.
[18] Chapter 6 Section 1 second paragraph of the Money Laundering Act and Chapter 6 Sections 14–17 of the Money Laundering Regulations.
[19] Operators that use automated systems could have reported that they have a manual monitoring system as well.

2. Does the company have a transaction monitoring system?

Number of companies

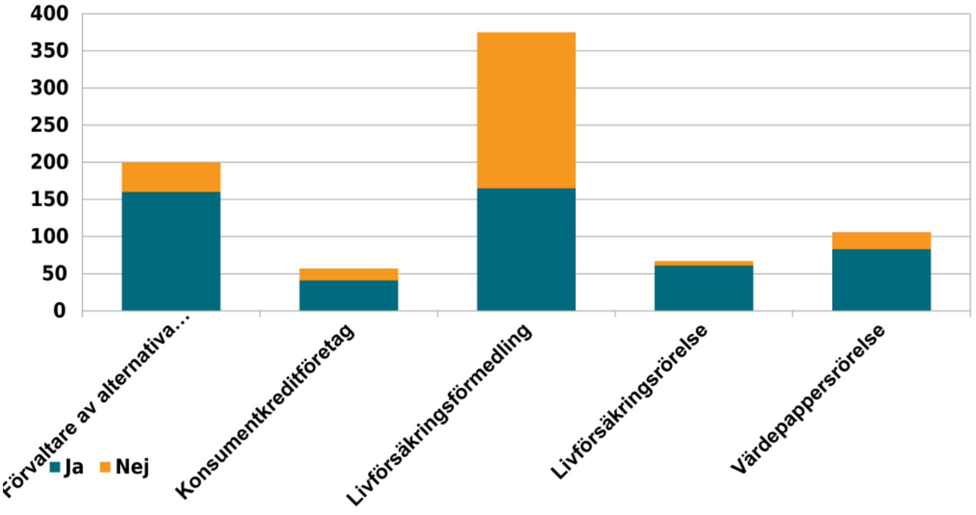


Source: FI

Note: This refers to 2020.

3. Does the company have a transaction monitoring system? (cont.)

Number of companies



Source: FI

Note: This refers to 2020.

The reported data reveals a link between a company that does not have a monitoring system and a lower number of suspicious activity reports to the Financial Intelligence Unit.[20] Only a few companies that reported that they do not

[20] See also Table 1 in the section 'Reporting to the Financial Intelligence Unit' below.

have a monitoring system also reported that had sent suspicious activity reports to the Financial Intelligence Unit in 2019 and 2020.

Conclusions

If a company does not carry out effective monitoring, it is difficult for them to detect, stop and report transactions that may constitute money laundering or terrorist financing. As stated above, there is no requirement for a company to apply an automated monitoring system. However, as there is a relatively low number of suspicious activity reports submitted to the Financial Intelligence Unit by companies that apply manual monitoring, FI believes there is a risk that the manual monitoring carried out by some companies does not sufficiently identify suspicious behaviour. Even for companies that apply automated monitoring systems, there is a risk that the alarms generated are not managed quickly enough to give either the company or the Swedish Police Authority a reasonable chance of stopping and following up the suspicious transaction.[21]

In conclusion, FI considers it problematic for companies to report that they do not have any systems in place at all to monitor transactions, either automated or manual. It is a legal obligation for a company to monitor ongoing business relationships and individual transactions, and if a company does not have a system (automated or manual), it will be difficult or impossible for it to detect, stop and report suspicious transactions. This is why the companies' transaction monitoring is an area that FI will monitor in its supervision for 2021 and will pay close attention to when following up the periodic reporting.

Reporting to the Financial Intelligence Unit

Introduction

If a company has reason to suspect that a customer is engaged in money laundering or terrorist financing, the company must report this to the Financial Intelligence Unit of the Swedish Police Authority. It is therefore important to have an effective and appropriate reporting structure in place to ensure that the system for combating money laundering and terrorist financing works properly.

Fact box – Reporting to the Financial Intelligence Unit

If an operator detects any atypical transactions, the operator must use enhanced customer due diligence measures and other necessary measures to assess whether there are reasonable grounds to suspect that money laundering or terrorist

[21] It is also essential for alarms to be managed quickly to enable the Financial Intelligence Unit of the Swedish Police Authority to use its option to freeze any funds that remain in an account.

financing is involved. If an operator has reasonable grounds to suspect money laundering or terrorist financing even before it starts its investigative measures, it does not have to carry out these measures. If the suspicion cannot be ruled out after an investigation or otherwise, the operator must report this to the Financial Intelligence Unit without delay.

A report must be submitted even if the operator chooses not to perform the transaction or if the business relationship is denied. However, the operator is only obliged to report transactions or activities to the Financial Intelligence Unit if it has reasonable grounds to suspect that the transaction may be connected to money laundering or terrorist financing.

Observations

Every year the periodic reporting provides FI with information about the number of suspicious activity reports for money laundering or terrorist financing that each company states that they have submitted to the Financial Intelligence Unit. Overall, the total number of reports submitted by the operators broadly confirms the statistics published by the Financial Intelligence Unit itself, which shows that the total number of suspicious activity reports continues to increase.[22] However, FI has noted that the ‘payment service companies’ sector differs in this respect from the other companies as the data on the number of suspicious activity reports given in the periodic reporting is much lower than in the statistics published by the Financial Intelligence Unit.

FI has noted that the number of reports per company differs significantly between the various sectors. In addition, FI has noted that some sectors that are typically considered to involve a higher risk, according to several national and international risk assessments,[23] are under-represented in this respect. Examples are payment services, which, inter alia, include companies that are authorised to carry out money transfers. The number of reports to the Financial Intelligence Unit submitted by registered payment service providers and payment institutions has been mostly constant, even though the number of companies in this sector increased significantly during this period.

The fact that the number of reports to the Financial Intelligence Unit differs between the various sectors does not necessarily mean that companies in the sectors with a lower number of suspicious activity reports are not complying with

[22] https://polisen.se/contentassets/f63b5e858a0349db9fffa9ce0a4ffce3/arsrapport-finanspolisen-2020.pdf
[23] Cf. e.g. The EU’s Supranational Risk Assessment Report and its annexes, SWD (2019) 650, pp. 79 and Penningtvätt – en nationell riskbedömning, pp. 22, https://www.fi.se/contentassets/0a11637dc8e941f69d0ede3f6b8b2b85/nationell_penningtv.pdf. An English translation is available.

the Money Laundering Regulations. This is because the sectors supervised by FI differ in several respects, particularly in terms of the number of customers and the kinds of products and services offered. However, FI has noted that the number of reports to the Financial Intelligence Unit varies within the various sectors and also between comparable companies. One consistent trend is that the number of reports of suspected terrorist financing is at considerably low levels.

Tabell 3. Reporting to the Financial Intelligence Unit

Number of reports

Sector	Money laundering 2019	Money laundering 2020	Terrorist financing 2019	Terrorist financing 2020
Banking or financing businesses	17,166	17,579	394	208
Other financial operations	703	630	226	20
Payment service providers	675	617	126	60
Life insurance businesses	171	397	411	4
Consumer credit companies	110	60	116	18
Securities businesses	13	19	23	2
Fund operations	7	12	25	0
Life insurance brokers	5	0	1	0
Housing credit companies	3	3	31	4
AIF managers	2	2	61	1

Source: FI

Note: Payment service providers refer to both registered payment service providers and payment institutions.

Conclusions

Reporting to the Financial Intelligence Unit has increased steadily in recent years and was 25% higher in 2020 than in 2018. The increase in the number of suspicious activity reports indicates a general increase in the knowledge and ability of operators, which FI sees as a positive step forwards. However, we have identified a risk for companies in sectors that are generally exposed to a high risk not reporting suspicious transactions to the extent that the increased risk would give cause to expect. In this context, FI would also like to stress the importance of submitting suspicious activity reports that are of good enough quality; this enables the Financial Intelligence Unit to investigate the suspected criminality effectively.