FI Supervision

Experiences from money laundering supervision 2016–2017

No. 1
12/04/2018

12/04/2018
Ref. 18-6701

TABLE OF CONTENTS

FI Supervision

Finansinspektionen publishes regular supervision reports in a numbered report series. The supervision reports are part of FI's communication. The reports describe the investigations and other supervision carried out by FI. Through these reports, FI presents its observations and assessments as well as its expectations in various matters. This information can support firms in their operations.

Summary

It is FI's assessment that firms in general have a greater awareness of the regulations than in previous investigations and are committing more resources to their work to prevent money laundering. But more needs to be done.

FI presents in this report its observations from the supervision of the regulations regarding measures against money laundering and terrorist financing[1] (money laundering regulations) conducted over the past few years.

During the period 2016–2017, FI investigated[2] the compliance of approximately 70 banks, savings banks, credit market companies and money remitters with the money laundering regulations. The investigations were based on the previous regulatory framework from 2009, but the conclusions and guidelines set out in the report also apply under the new regulations that were introduced in 2017.

FI makes the assessment that the firms in general have established systems, procedures and documentation, but in several cases, they had deficiencies in their analyses, assessments, follow-up and measures.

FI also makes the assessment that the firms' work to prevent money laundering and terrorist financing has improved in recent years. An area where the firms could further improve is to ensure that internal regulations and processes have been clearly tailored to their operations and have the intended effect. The work to prevent money laundering and terrorist financing must be continuous. In order for such efforts to have an impact, the entire chain of measures needs to be connected and constantly updated based on changing conditions. This is also a prerequisite for a monitoring system to be effective.

FI noted that the firms' general risk assessment does not always sufficiently identify the risks for all types of customers, products, services and distribution channels.

FI's investigations also showed that the firms do not always take sufficient measures to fulfil the customer due diligence requirements. For example, in several cases there was no information about the purpose and nature of transactions, risk classification of customers and beneficial owner.

Deviant behaviour or transactions that raise suspicions about money laundering must be reported to the Financial Intelligence Unit of the Swedish Police. FI noted that the firms' monitoring systems were not evaluated on a regular basis, which is necessary to identify and report deviant behaviour and transactions to the desired extent.

---

1 Money Laundering and Terrorist Financing (Prevention) Act (2009:62) and FI's regulations and general guidelines (FFFS 2009:1) on measures against money laundering and terrorist financing. After 1 August 2017, the Anti-Money Laundering and Terrorist Financing Act (2017:630) and Finansinspektionen's regulations (FFFS 2017:11) regarding measures against money laundering and terrorist financing.

2 Clarification 2018-12-07: The term *investigations* in this report refers to formal investigations, surveys and other supervision activities.

What has FI investigated?

In the period 2016–2017, FI has carried out over seventy investigations looking at how financial firms are complying with the money laundering regulations. These investigations have mainly been focused on firms' work with risk assessments, customer due diligence, monitoring and reporting of suspicious transactions.

The investigations encompassed major banks, small and medium-sized banks, money remitters and credit market companies.

Fi has conducted these investigations by gathering written materials, including random samples of risk assessments and measures implemented with respect to individual customers, as well as on-site visits featuring interviews with managers and administrators at these firms. The documentation that has been reviewed consists of internal guidelines and instructions, company-wide and individual risk assessments, customer due diligence, transaction monitoring and reports to the Financial Intelligence Unit.[3]

RISK ASSESSMENT

According to the regulations, firms must assess the risk of the products and services they offer being used for the purposes of laundering money or terrorist financing. Firms also have to assess the size of this risk. This is called the general risk assessment. In addition to its general risk assessment, the firm also has to assess the risk associated with the individual customer and business relationship.

CUSTOMER DUE DILIGENCE

Firms have to put measures in place to ensure customer due diligence is conducted when business relationships are established in order to enable them to have good knowledge of their customers. A business relationship denotes a commercial relationship that is expected, at the time it is established, to have a certain permanence, but this can also arise though the parties' actions.
The documentation that has been collected and information about what measures have been put in place for the purposes of customer due diligence has to be stored securely by the firms. If there is a high risk of money laundering or terrorist financing, the firm has to implement more rigorous measures.

MONITORING AND REPORTING

Firms have to monitor their business relationships and transactions in a way that enables them to detect any activities and transactions that may be suspected of constituting an aspect of money laundering or terrorist financing. If, following more detailed analysis, the suspicion remains, information about all circumstances that may be suggestive of money laundering or terrorist financing has to be reported to the Financial Intelligence Unit without delay.

3 Financial Intelligence Unit denotes the Financial Intelligence Unit of the Swedish Police Authority, which receives, processes and analyses information concerning suspected money laundering and terrorist financing in accordance with the Anti-Money Laundering and Terrorist Financing Act (2017:630).

What has FI found in the investigations?

Firms' general risk assessments are a cornerstone of the fight against money laundering and terrorist financing . Firms must always work on the basis of the risks associated with their operations and implement appropriate measures to reduce the risks identified. On the basis of its experience from the investigations conducted during the period in question, FI has noted that there are shortcomings in several areas, which these firms therefore need to improve.

THE GENERAL RISK ASSESSMENT

FI has seen that there are many methods used to draw up a general risk assessment. Many firms draw up the general risk assessment themselves, others, mainly smaller firms, get outside assistance. FI has also seen that it is common for a firm that is part of a larger group to allow the parent company to draw up a risk assessment that all the firms in the group then use as their own. It may also, for example, be a partner firm that draws up the risk assessment. When a company does not draw up the risk assessment itself, there is a major risk that the risks that are particularly important for that specific firm are missed.

FI has also noted that it is not always stated clearly how firms conduct assessments of how their operations can be used for the purposes of money laundering and terrorist financing. It is important that the firm surveys and assesses the risks for all types of customer and all types of product, service and distribution channel it offers. Geographical factors also have to be taken into account. In addition, the risk assessment also has to take into account the methods, trends and patterns that may be used in money laundering. There has to be a clear description of how the evaluation of risk has been conducted. The consequences of not conducting a thorough survey are that the firm will not be able to form an accurate view of the way in which it could potentially be used for the purposes of money laundering. In turn, this will prevent the firm from putting appropriate risk-reduction measures in place when classifying the risk of customers, when conducting customer due diligence or when monitoring suspicious transactions and anomalous behaviour.

FI has noted that several firms have not had a specific assessment of how they may potentially be used for the purposes of terrorist financing. The risks of being used for the purposes of terrorist financing are different from the risks associated with money laundering and it is therefore important that firms describe, identify and manage these different risks separately.

INDIVIDUAL RISK ASSESSMENT OF THE CUSTOMER

The customer due diligence measures firms are to implement have to be tailored to the customer's individual risk. A customer that is assessed as high risk requires more extensive measures than a customer that is assessed as normal or low risk.

FI's experience shows that firms have not tailored their customer due diligence measures on the basis of the risk associated with the customer to a sufficiently high degree. FI has found examples of situations in which customer due diligence information has actually been collected, but not all of the relevant information about the customer has been taken into account when assessing the customer's risk. In one other example, a firm had not assessed the risk of an individual customer as high, while the company of which this person was the beneficial owner – i.e. the person who ultimately controlled the company – was classified as high risk. FI is of the opinion that in this case the firm should have also classified the individual customer as high risk. There have also been cases where customers have not been assigned any risk classification at all, in spite of the business relationship having been ongoing for several years and there being plenty of information about the customer.

CUSTOMER DUE DILIGENCE MEASURES

If firms are to make it more difficult for their operations to be used for the purposes of money laundering or terrorist financing and prevent this, they must have good knowledge of their customers and of their customers' business affairs.

FI's investigations have shown that firms do not always have sufficient customer due diligence measures in place. It has been found that there is a lack of information about the purpose and nature of the business relationship in the firm's customer files, or that the documentation is inadequate. This also applies to information about which products and services the customer is using. In several cases, there has been a lack of information about beneficial owners or what risk classification the customer has been given.

FI's investigations have shown that some firms have not tailored their customer due diligence measures to a sufficiently high degree to the real risks associated with the customer. In some cases, this has been due to an erroneous or non-existent classification of the risk of the products and services a certain customer has used, which has led, in turn, to an erroneous classification of the customer's risk. In other cases, the firm, in spite of the customer being assessed as high risk, has not tailored its customer due diligence measures accordingly. For example, information about the source of the wealth and/or assets has been absent for certain high-risk customers. Insufficient customer due diligence entails a risk of transaction monitoring being less effective because an erroneous view may be used as the basis for this monitoring. This also increases the risk of the firm being used for the purposes of money laundering and terrorist financing.

PURPOSE AND NATURE ARE CLEAR AND UP TO DATE

Collection of that which is defined in the money laundering regulations as *the business relationship's purpose and nature* is the key to being able to manage the risks associated with a customer and to monitoring the customer's transactions.

The scope of firms' descriptions of purpose and nature – for example information about which products and services the customer intends to use and the size and frequency of future transactions, as well as, in the case of business customers information about the customer's business activities – has to be proportionate to and adapted to the risks associated with the customer. A frequent shortcoming FI has seen is the purpose of the business relationship being described in only a few words. For example, words such as "private banking", "foreign payments", "wealth management" and "cash management" have often been used.

FI has also seen examples of inadequate documentation of the purpose of the business relationship. In one case, there was a beneficial owner who appeared in three different business contexts and where all of the customers were foreign companies. The purpose of these business relationships was listed as managing funds from the sale of shares, but there was no information about why the three companies were needed or about what role the representatives or authorised signatories had, as these people had no obvious or natural link to the companies.

Firms must tailor the scope of the information that is gathered about purpose and nature to the individual customer and the risks associated with them. The information has to provide a sufficiently good description so that the purpose and nature of the business relationship is clear. This is particularly important for customers who have been assessed as high risk. A far too broad and generalised description and documentation of the purpose of the business relationship risks leading to the firm not fully understanding the risks associated with the customer's business activities. This also entails a risk that firms will not be able to conduct accurate ongoing follow-up of the business relationship and thus will not be able to monitor the customer's transactions in a satisfactory manner. This increases the risk of transactions and behaviours which could be an aspect of money laundering or terrorist financing not being detected and reported to the Financial Intelligence Unit.

MANAGING AND DOCUMENTING CUSTOMER DUE DILIGENCE DATA

It is common for firms to use some form of electronic system for managing and documenting the customer due diligence information that is collected. In some cases, an overarching system is complemented by several other systems. There are also examples of physical customer files being used to complement an electronic system in which other aspects of customer due diligence are stored. Aside from electronic systems and customer files, information about certain circumstances or details about the customer are held by the account manager, cashiers or similar. FI has noted that all information about the customer is not always documented and kept together in one place. The fact that customer due diligence information is spread across several systems, functions and positions can lead to a situation in which it is not easy to produce and identify documents and data pertaining to customer due diligence. This also increases the risk that important information is overlooked, for example when continuously following up business relationships and when monitoring transactions.

One example of inadequate documentation of customer due diligence data that FI has observed in its supervision concerned a customer domiciled in a country that the firm classified as a high-risk country. The firm believed that the customer due diligence conducted was sufficient because the structure and format was "generally accepted". Fi believes that this approach entails a risk because it is *not* necessarily the case that that which is regarded as "generally accepted" for a specific department within a firm is also seen as such by all employees, for example the staff who review transactions and activities and need access to relevant information in order to enable them to conduct an accurate analysis.

WHEN IS A BUSINESS RELATIONSHIP ESTABLISHED?

Firms have to implement customer due diligence measures when a business relationship is established. The concept of *business relationship* applies to all undertakings encompassed by the money laundering regulations. The term 'business relationship' denotes a commercial relationship that is expected, at the time it is established, to have a certain permanence.

An established business relationship can also arise when a customer returns to the firm and conducts occasional transactions. In such cases, the business relationship has been established through the actions of the firm and the customer. This means that money remitters, currency exchangers and other similar businesses, which are often characterised by a large number of small and recurrent transactions, also need to define when a business relationship actually arises in their operations. FI is of the opinion that, in any case, a business relationship is established when transactions are conducted by the same person and with a frequency of twelve times over a period of twelve months. This type of frequency is a strong indication that the business relationship is recurrent and thus also permanent. Customer behaviour of this nature differs considerably from a customer who uses the firm occasionally in order to conduct their transactions.

The firms offering products and services associated with a high level of risk may need to use a narrower definition of the term 'business relationship' in order prevent the firm being used for the purposes of money laundering, especially in its contact with high-risk customers. One example of a high-risk customer is people who frequently exchange or send large amounts that are close to the firm's threshold.

TAILORING MONITORING TO SUIT CUSTOMER RISK

The practical implication of the obligation to conduct monitoring is that larger firms, which have complex operations, a large number of products, services, customers and transactions, should have automatic monitoring systems in place. This is necessary if they are to be able to monitor all the transactions that take place automatically or remotely without any manual processing on the part of the firm. An automatic monitoring system is required in order to enable the detection of instances where a customer's behaviour departs from what is expected on the basis of the customer due diligence conducted by the firm. Among small firms, with less complex operations, fewer products, services and transactions and customers whose transactions take place manually (e.g. cash-intensive businesses), it is common for monitoring to be conducted manually. Regardless of which system is in place for monitoring activities and transactions, it is important that monitoring is continuous in order to enable any anomalous activities and associated transactions to be detected.

In the same way that customer due diligence measures have to be tailored to the assessed risk of money laundering, the monitoring of transactions also has to be tailored to the applicable risk. For example, customers and transactions that are high risk therefore have to be monitored more carefully than those that are low risk.

As part of its investigations, FI has examined transactions that have been carried out by firms' customers. This has revealed a number of transactions that FI believes should have resulted in suspicions concerning money laundering. FI, which also has a reporting obligation pursuant to the Anti-Money Laundering Act, has, within the scope of these investigations, reported transactions deemed to be suspicious to the Financial Intelligence Unit. This shows that there are shortcomings in firms' monitoring of transactions and their reporting to the Financial Intelligence Unit. These shortcomings may be due to factors such as the firms' monitoring systems not being tailored to the assessed risks of their operations or the alarms that have been generated not being investigated sufficiently thoroughly. At the same time, it is important not to report too much and indiscriminately. It is important that reports made to the Financial Intelligence Unit are relevant and of a consistently high quality. If not, the Financial Intelligence Unit will be drowned in meaningless reports, which will harm the effectiveness of the unit's work.

NEW ASSESSMENT WHEN REPORTING TO THE FINANCIAL INTELLIGENCE UNIT

When an activity or transaction is reported to the Financial Intelligence Unit, the firm has to conduct a new assessment of the customer to which the report pertains. The customer's risk classification has to be revised on the basis of the information in the report submitted and enhanced customer due diligence measures have to be implemented. Another measure that may be appropriate is increasing the frequency at which the customer's transactions are monitored so that the customer's risk can be managed by the firm. The firm may also need to consider whether it should terminate the business relationship with the customer, which may be necessary in some cases in order to enable the firm to manage the risk.

The data that is included in reports to the Financial Intelligence Unit concerning suspicious transactions are also important in other contexts. The firm has to take into account data that has been reported to the Financial Intelligence Unit when the firm is assessing, as part of the general risk assessment, how the products and services it supplies may be used for the purposes of money laundering. These reports are an important source of data for the firms when they are drawing up or updating their general risk assessments. The same applies to firms' individual risk assessments of customers.

Criminal investigation authorities can contact firms and request data about their customers. These requests may pertain to both victims and perpetrators. A request of this type may indicate that a customer is in some way of interest from the perspective of money laundering or terrorist financing.

EVALUATING THE FIRM'S MONITORING SYSTEM

Firms' monitoring systems generally raise the alarm about suspicious transactions on the basis of predetermined parameters and rules. Each firm has

to tailor the scenarios in its monitoring system to the business it conducts. If the alarms that are raised in the system are rarely reported to the Financial Intelligence Unit, this may indicate that the system is not sufficiently tailored to the firm's business. The same applies if alarms are being reported too frequently. Too many alarms may mean that alarms are not been investigated sufficiently thoroughly before being reported to the Financial Intelligence Unit. On the other hand, too few alarms may indicate that suspicious transactions are not generating alarms. All in all, a poorly calibrated monitoring system entails a risk that suspected money laundering and terrorist financing are not being detected and reported to the Financial Intelligence Unit. Consequently, it is important that firms monitor transactions and activities carefully and that reporting to the Financial Intelligence Unit takes place so that it is possible to detect and investigate potential crimes.

In its investigations, FI has seen that firms' monitoring systems are not always adjusted to the risks identified by the firm and to its business activities. If a monitoring system is to be effective, the firm needs to regularly evaluate the system. If a certain scenario generates no or very few alarms, the firm must evaluate whether the scenario is actually needed or if the parameters on which the scenario is based need to be adjusted. The same applies to scenarios that generate a large number of alarms, few or none of which lead to a suspicion that is reported to the Financial Intelligence Unit.

Conclusions

There is much that has been improved in terms of firms' work to combat money laundering and terrorist financing, but more needs to be done. If firms are not managing the risks correctly, damage can be done to both individual firms and the financial system as a whole.

Many firms have the internal regulations in place that are required in order to comply with the various requirements in the money laundering regulations. Nonetheless, there is a need for firms to redouble their efforts in this respect in order to ensure that internal procedures, guidelines, monitoring systems, etc. are explicitly tailored to their business activities and have the intended effect.

Firms' efforts to prevent money laundering and terrorist financing are a process that continues constantly, all aspects of which are interlinked. The various aspects described by FI in this report are all essential if these efforts are to have the desired result. Here follows a description of the improvement measures for firms that FI has identified and will be following up in its supervision.

- The risk assessment has to be tailored to the firm's business, which is why it does not work when, for example, one firm simply copies another's general risk assessment. Differentiate between assessment of the risk of money laundering and terrorist financing.
- Ensure that an individual risk assessment is conducted for all customers (low, medium, high).
- Describe the purpose and nature of the business relationship in more detail, especially when the customer is more complex or has a higher risk.
- Tailor customer due diligence measures and the monitoring system on the basis of the information collected and risks identified (both of the firm and of the customer). Ensure that information is kept together in one place and is easy to produce.
- Be aware that a business relationship arises when the same person carries out several transactions in a certain period – a rule of thumb is twelve transactions in a twelve-month period. However, fewer transactions in such a period may constitute a business relationship in certain cases.
- Ensure that the monitoring system is tailored to the firm's business and risks. This contributes to more accurate reporting to the Financial Intelligence Unit.

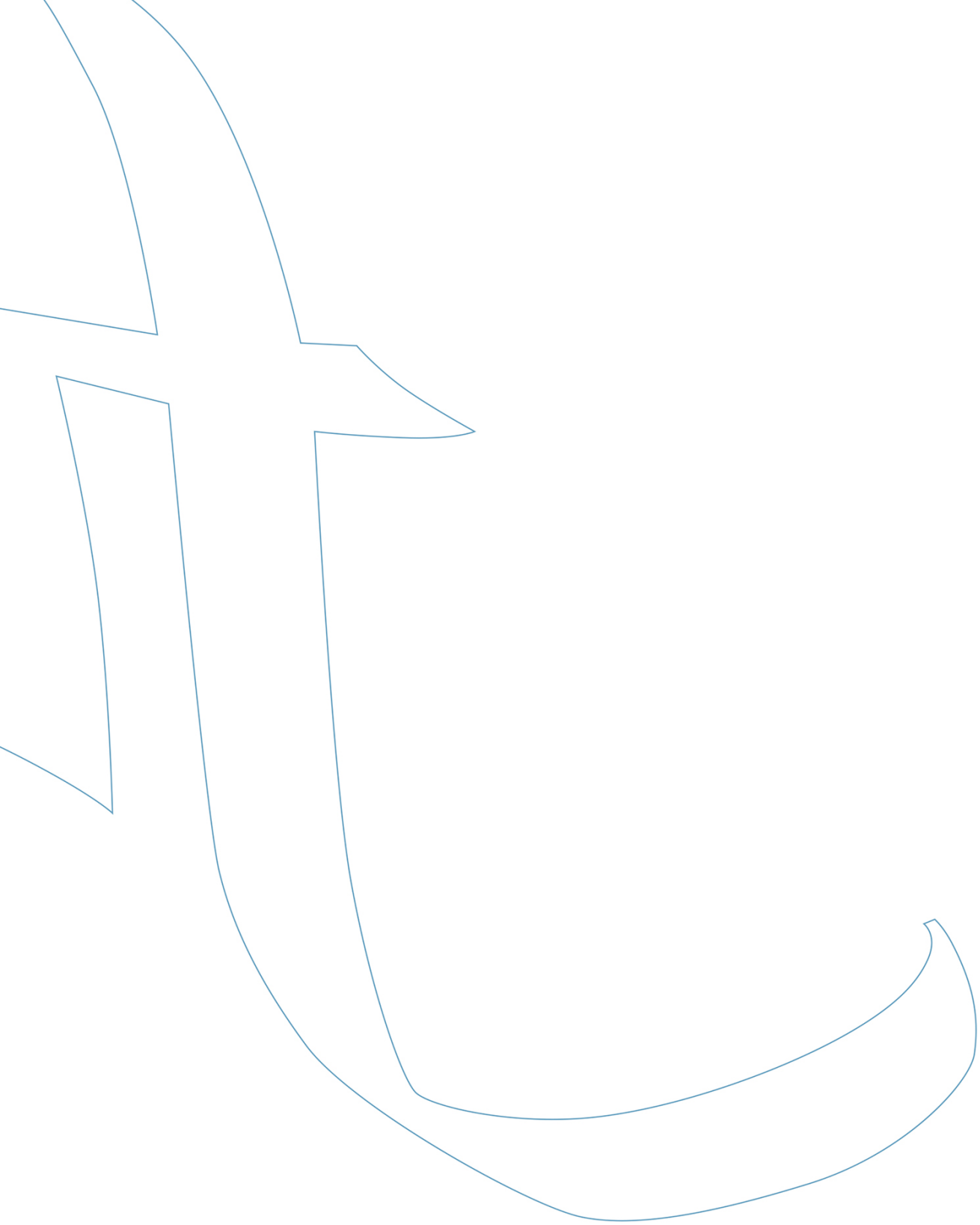
The consequences of firms failing to adequately manage the risks associated with money laundering and terrorist financing are serious – this makes it possible for criminals and terrorists to exploit the financial sector for their purposes. If firms are instead doing a good job in this respect, this can help society to fight and prevent crime and terrorism.

FUTURE SUPERVISION

FI works continually to inform firms and the general public about the rules that apply. In 2017, for example, FI published extensive information about the new money laundering regulations on its website.

In the Government's budget for 2018[4], FI has been allocated specific funding that is intended to enhance supervision in order to combat money laundering and terrorist financing . Consequently, FI's ambition is to increase its supervisory measures within this area in the years ahead. An important tool in FI's risk-based supervision is the periodic reporting that was introduced in 2018 and encompasses all firms that are subject to FI's anti-money laundering supervision. The data obtained through periodic reporting forms the basis of FI's risk classification of firms. Risk classification is an important tool that enable FI to target its supervisory measures at the areas in which the risks are deemed to be higher.

4 http://www.regeringen.se/4a65cf/contentassets/79f6d27416794f0bb146c792e02b65fc/utgiftsomrade-2-samhallsekonomi-och-finansforvaltning.pdf, p. 74



Finansinspektionen
Box 7821, 103 97 Stockholm
Besöksadress Brunnsgatan 3
Telefon +46 8 408 980 00
Fax +48 8 24 13 35
finansinspektionen@fi.se

www.fi.se