Information for businesses on money laundering and terrorist financing

Report suspected money laundering and terrorist financing

THE COORDINATING BODY FOR ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM

This brochure is intended to provide business owners, so called operators, with information on how your business may be exploited for the purposes of money laundering and terrorist financing. It is primarily intended for those who run a business that is covered under the scope of the Anti-Money Laundering Act and who are under the supervision of the county administrative board. This applies, among other things, to those who engage in business providing accounting or auditing services, as well as independent lawyers, tax consultants, company formation agents, business brokers and business centre or postbox service companies. The brochure provides information on how to report to the Financial Intelligence Unit and the risks that are associated with your particular area of business.

The information provided is intended to increase your knowledge and the knowledge of other operators with regard to money laundering and terrorist financing. Here, we describe certain situations and red flags that may indicate that your business is being used to launder money or finance terrorism.

This information is provided by the Coordinating body for anti-money laundering and countering financing of terrorism. The information has been produced by the Financial Intelligence Unit and by the county administrative boards of Skåne, Stockholm and Västra Götaland counties, which act as the supervisory authorities for your business.

The Coordinating body is led by the Swedish Police Authority and consists of 17 members. We serve as a forum for information exchange and knowledge transfer. Our assignment is to identify, map and analyse risks and methods for money laundering and terrorist financing in Sweden. We also work to inform operators about how they can prevent their businesses from being used for money laundering or terrorist financing.

Information for other operators can be found on the website **polisen.se/penningtvatt**. Here you will also find more information about the Coordination body.

Published by: The Swedish Police Authority:
Registration number: A633.801/2021
Version: October 2021
Graphic form: Blomquist Communication, blomquist.se
Photo: Alvin Mahmudov p. 1, Getty p. 3, Police Image Bank p. 6, Clay Banks p. 11.

You are obliged to report to the Financial Intelligence Unit

Under the Anti-Money Laundering Act, you as an operator are obliged to review and, in case of suspicion, report transactions and activities to the Financial Intelligence Unit in order to make it possible to detect money laundering or terrorist financing. You are also obliged to have a system in place that allows you to provide information on whether you have had a business relationship with a particular customer during the past five years, and in such cases, the nature of the business relationship.

When you report a suspected individual or activity, law enforcement authorities, such as the the Swedish Police Authority, the Swedish Economic Crime Authority, the Swedish Tax Agency or the Swedish Prosecution Authority may solve crimes that otherwise would not have been discovered.

If anything about your customers' transactions or activities seems suspicious, you must perform a review. If you still have suspicions after your review, you must report it to the Financial Intelligence Unit, which is part of the Swedish Police Authority.

How to report

In order for you to be able to submit a report to the Financial Intelligence Unit, you must register your business and register as a user in the IT system goAML. Registration in goAML can take up to two working days to be finalised, so it is a good idea to register as a user even before you have something to report. As a registered user, you will receive relevant information from the Financial Intelligence Unit and can ask questions.

The web portal contains manuals for registration and reporting in goAML as well as other material you will need to get started. The Financial Intelligence Unit recommends that you read these manuals before registering as a user.

Questions about goAML

Answers to most of the questions you might have can be found in the manuals and other material that you will be able to access after you register. If you have questions that are not answered in the material, you can contact fipo@polisen.se.

The website for goAML is **https://fipogoaml.polisen.se**

You are obliged to refrain from performing suspicious transactions

Under the Anti-Money Laundering Act, you as an operator are obliged to prevent the risk that you will be used as a tool for criminal activity. You are therefore obliged to refrain from carrying out transactions that could be suspected money laundering or terrorist financing.

If it is not possible to refrain from conducting a suspicious transaction, you may carry out the transaction in exceptional cases. This applies, for example, when suspicion arises after the transaction has been completed and it is not possible for you as an operator to cancel the transaction. Or, it may be that due to another law or equivalent, you are unable to prevent a certain transaction from being completed or that a further investigation would be made more difficult if you refrain from conducting the transaction.

In these cases, you must submit a suspicious activity report immediately afterwards to the Financial Intelligence Unit. Your reporting obligation continues to apply even if the transaction is cancelled or the business relationship is terminated.

If you refrain from completing the transaction due to the suspicion of money laundering or terrorist financing, the circumstances on which suspicion is based must be reported to the Financial Intelligence Unit.

Money laundering is the act of concealing the connection between criminal acts and money or other property. This may include, for example, money obtained from drug offences, tax offences or fraud that is "laundered" in order to be used in the legitimate financial system.

Terrorist financing concerns the concealment of what a sum of money is to be used for and involves the financial support of terrorism by collecting, providing or receiving money or other property that is intended to finance terrorism.

When are you obliged to report to the Financial Intelligence Unit?

If you suspect money laundering or terrorist financing, you must report this to the Financial Intelligence Unit immediately. You do not have to have evidence that money laundering has in fact occurred, a low degree of suspicion is enough. As an operator, you may not inform the customer or any third party that you are reviewing a transaction or that you have submitted a report to the Financial Intelligence Unit.

What needs to be included in the report and how should I submit a report?

Any report submitted to the Financial Intelligence Unit must contain information on all the circumstances surrounding the suspected activity that may indicate money laundering or terrorist financing.

The Financial Intelligence Unit needs a thorough description of the suspected activity, in order to be able to investigate a report. It is very important that the reports submitted are accurate and thorough if the Financial Intelligence Unit is to be able to investigate and assess suspected money laundering and terrorist financing activities.

If you have documentation that confirms the information in your report, you must include this documentation. This documentation can be, for example, an account statement, an ID document, an agreement or a receipt. You must also be prepared to submit information, without delay, about whether you have had a business relationship with a particular person in the past five years. It is therefore important that you save all of your documentation and information about your customers in an orderly manner.

All information about what must be contained in the report can be found at goAML.

What happens after I submit a report?

The Financial Intelligence Unit assesses the information in the report to investigate whether there may be suspicion of money laundering or terrorist financing. Information in a submitted report can form part of an intelligence file where crimes can be discovered by law enforcement authorities.

The suspicious activity report that you submit may be the crucial piece of information that makes it possible to detect money laundering or terrorist financing. In cases of suspected terrorism, the Financial Intelligence Unit sends an intelligence file immediately to the Swedish Security Service for assessment and investigation.

Will anyone find out that you as an operator have submitted a suspicious activity report?

The Financial Intelligence Unit will not inform the person being reported that a report has been submitted or who has submitted the report. The identity of individuals who submit suspicious activity reports to the Financial Intelligence Unit is subject to secrecy.

You may be guilty of money laundering and terrorist financing

If you as an operator participate in an activity that can be assumed to have taken place to conceal the criminal origins of money or other property or to assist (facilitate) someone else in the acquisition of such property, you risk being convicted of a crime under the Act on Penalties for Money Laundering Offences (2014:307).

To be criminally liable, you do not have to be aware that the money originated from criminal activities; it is sufficient that you should have realised it. This means that if you fail to fulfil your obligations under the Anti-Money Laundering Act, including monitoring and control of transactions, you may risk being convicted of a crime leading to a fine or imprisonment for, among other things, commercial money laundering.

The Act on Criminal Responsibility for the Financing of Particularly Serious Crimes in Certain Cases (2002:444) stipulates that it is prohibited to collect, provide, or receive money or other property in certain cases. This is because, in these cases, the purpose of the property is to support terrorist activities (or the knowledge that it will be used for terrorist activities). This means that an individual is guilty of financing terrorism if he or she transfers money or other property to people who are planning or actively engaged in carrying out terrorist crimes. The assets do not need to be used specifically in connection with a terrorist attack.

Be vigilant!

The following examples of red flags may provide you, as an operator, a reason to do an in-depth review of a customer and the customer's transactions or to refrain from completing a transaction altogether. This holds especially true when there are several red flags at once or they recur over time. This does not have to mean that something illegal has in fact occurred, just that you as an operator may need to review the transactions more closely.

1 Red flags linked to customer behaviour

- The customer is nervous or acts in a threatening manner.
- The customer tries to develop close relationships with employees.
- The customer seems to be acting on behalf of a third party, but does not reveal this information.
- The customer has an unusual lack of knowledge regarding their business.
- The customer seems unusually interested in internal control systems as well as customer due diligence routines and reporting.
- The customer acts defensively when completing customer due diligence measures or overemphasises the justification of certain transactions.
- The customer has an unusually high level of knowledge about anti-money laundering laws.

2 Red flags linked to the customer's identity

- It is difficult to verify the identity and/or contact details of the customer or the customer's representative.
- Identity documents or documents proving income cannot be verified or are in a foreign language.
- The customer is unwilling to have personal contact with you and wishes to conduct the business relationship in another way, for example, through intermediaries.
- The customer discontinues the business relationship after being asked to submit identity documents.
- The customer spells his or her name differently or presents different identity documents on different occasions.
- The customer is being observed or monitored by other people.
- The customer's contact details are incomplete or unclear.
- The customer has a home or business telephone number that is often switched off or does not exist.
- The customer changes addresses repeatedly.
- The customer does not want post sent to his or her home address.
- The documentation provided by the customer does not correspond to the information the customer has otherwise submitted.
- The customer is established in a country outside the EEA that the EU Commission has identified as a high-risk third country.
- The customer or the customer's beneficial owner is a person in a politically exposed position (a Politically Exposed Person or PEP), or is a family member or known employee of such a person.
- The customer's representative has previously been involved in several short-lived companies.
- The customer uses frontmen or people who act as the company's representatives, even though they do not really work for the company.

3 Red flags linked to payment methods and business schemes

- Unusual business situations, such as engaging in commerce in deviant jurisdictions or with deviant counterparties as well as a high degree of cash use compared to what would be considered normal.
- Unusual transactions for the customer's business areas or unclear receipts/accounting documents.
- The customer's behaviour and business do not match with the information previously provided.
- The customer insists that the business relationship be established unusually quickly.
- The customer is unable to provide information about the origin of funding.
- Payments are made through a representative.
- The customer wants to make payments using large amounts of cash and does not provide a good explanation regarding the source of the money.
- Anything that is unusual for business, whether it be deviant counterparties, commerce within deviant jurisdictions, high rates of cash use compared to what would be expected in the sector, etc.

Examples of approaches

All types of crime that can result in financial gain can be so-called predicate offences for money-laundering. In order to launder money, the criminal needs to introduce the proceeds of criminal activities into the legitimate financial system. A common approach is to start and use companies as a tool to make money from criminal activities appear legitimate. Common crimes where companies are used in this way are, for example, tax offences, accounting crimes and fraud.

In order to conceal the origin of the money and create an impression of legitimacy for the company, criminal proceeds can be divided and transferred between several different accounts, preferably across several jurisdictions. International organisations such as the Financial Action Task Force (FATF) and the Organisation for Economic Co-operation and Development (OECD) have identified major risks associated with cross-border commerce.

The approaches used may differ depending on the kind of business you are involved in. Below are some examples that will help you as an operator better understand how and when your business, or your products and services, can be used as part of a money laundering scheme or terrorist financing.

Business centre and postbox service companies

A risk associated with these business areas is the potential for anonymity that is attractive in a money laundering or terrorist financing scheme. It is therefore important to perform adequate customer due diligence measures in this context. One example of a red flag could be that several companies or individuals are registered in the same postbox. Another example could be a case where companies listed at business centre or postbox service companies provide insufficient information about the company's representatives. It can then be difficult to investigate and determine who the company's representative is. Other examples include when the same representative returns to represent new companies or if the same representative has many different companies. This applies regardless of whether the same postbox is used or not.

Accounting and auditing services

These services can be used as a seal of approval for financial statements for businesses that have been used as part of a money laundering scheme or the financing of terrorism. Accounting and auditing services can be used to legitimise illegal transactions and to make false documents and invoices appear to be correct.

From the outside, the customer's company may appear to be engaged in legal operations when in fact it is being used for VAT fraud, withdrawal of cash for payment of undeclared labour, transfer of profits to the accounts of criminal actors or to enter criminal money into the company's accounts as turnover.

Insufficient customer due diligence measures or a lack of understanding of the customer's operations can cause accounting and auditing services to fail to detect transactions that should arouse suspicion for reporting to the Financial Intelligence Unit. Such suspicious transactions include:

- Money from criminal activities is recorded as a sale and then converted into legal funds in the form of salaries and dividends.
- Legally obtained money is paid as wages for undeclared labour or for private consumption.
- Money enters the customer's company account for no reason, the company owner is asked to repay the money (the payer cites payment error) but pays to an account other than the account where the money originated.
- The operator notes a larger amount of money coming into a customer's account without documentation to show where the money came from.
- The customer issues or pays false invoices.
- Cross-border payments.

Tax Consultants

These businesses can be exploited to carry out tax schemes where money from criminal activities is introduced into the legitimate financial system.

Large sums of money can be laundered through complex cross-border schemes that are difficult to investigate. This can be part of number of money laundering schemes with varying degrees of complexity.

Independent lawyers

An independent lawyer can be exploited by establishing agreements that legitimise illegal transactions. This can be a part of a number of schemes with varying degrees of complexity. By assisting with financial transactions, an independent lawyer may contribute to money laundering by moving illegal funds and making them appear legitimate. In much the same way, an independent lawyer can, through his or her participation in the transfer of real estate, companies and assets, make them appear legitimate. This can involve a number of money laundering schemes with varying degrees of complexity.

One such scheme is a case where the client seeks to use the lawyer's client funds account to carry out transactions covered by the assignment. For example, it could be about transferring funds to a third party.

Another example is the creation of a fictitious company structure within the framework of an otherwise legal and “normal” assignment. In order to prevent the business from being exploited for the purposes of money laundering, the independent lawyer must have a good understanding of each individual transaction, action or circumstance within the scope of the assignment.

Sham litigation can also be used as a means to obtain a judgement or decision that allows money to be used and transferred from one actor to another with the assistance of the authorities. This gives the transfer the appearance of legitimacy and the person who is laundering the funds can show the origin of the money.

Company formation agents and business brokers

Companies engaged in criminal activities can be integrated into legal businesses through the acquisition of established companies. This allows

them to gain access to attractive customers and markets, to operate anonymously and to act through established companies with a good reputation. During acquisition, money from criminal activities can be laundered and used as payment.

An individual who has acquired a company can put other people on the board, who can also be frontmen in other contexts. An individual or individuals who have acquired a company or serve as its representatives may also have a history of several other acquisitions that have been declared bankrupt. The company's share capital may come from criminal activities. In the case of acquisition from the company founder, money is laundered by financing the purchase with money obtained from criminal activities.

More information

Information about the risk assessments, routines and guidelines that you need to use in your business can be found on your county administrative board's website. If you have any questions regarding your obligations under the Anti-Money Laundering Act or about this brochure, please contact the county administrative board that conducts supervision for your business. The county administrative board responsible for supervision of your business is determined by which county your business has its registered office. See image on next page.

The information provided in this brochure is based, among other things, on the following regulations:

- Act on Measures against Money Laundering and Financing of Terrorism (2017:630), the Anti-Money Laundering Act
- Act on Penalties for Money Laundering Offences (2014:307)
- Act on Criminal Responsibility for the Financing of Particularly Serious Crimes in Certain Cases (2002:444)
- The Swedish Police Authority's regulations on reporting and submission of information in accordance with the Anti-Money Laundering Act (2017:630) (PMFS 2020:3, FAP 499-1)
- The County Administrative Boards' regulations and general guidelines on measures to prevent money laundering and terrorist financing (12FS 2019:29, 01FS 2019:53 and 14FS 2017:178, 14FS 2018:51 and 14FS 2019:52).

Länsstyrelsen Skåne

Blekinge County
Jönköping County
Kalmar County
Kronoberg County
Skåne County
Östergötland County

Länsstyrelsen Stockholm

Gotland County
Jämtland County
Norrbotten County
Stockholm County
Södermanland County
Uppsala county
Västmanland County
Västernorrland County
Västerbotten County

Länsstyrelsen Västra Götaland

Dalarna County
Gävleborg County
Halland County
Västra Götaland County
Värmland County
Örebro County

The County Administrative Board of Skåne
Switchboard: 010-224 10 00
E-mail: skane@lansstyrelsen.se
More information is available at:
lansstyrelsen.se/skane/samhalle/penningtvatt

The County Administrative Board of Stockholm
Switchboard: 010-223 10 00
E-mail: stockholm@lansstyrelsen.se
More information is available at:
lansstyrelsen.se/stockholm/samhalle/penningtvatt

The County Administrative Board of Västra Götaland
Switchboard: 010-224 40 00
E-mail: vastragotaland@lansstyrelsen.se
More information is available at:
lansstyrelsen.se/vastra-gotaland/samhalle/penningtvatt

THE COORDINATING BODY FOR ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM

Länsstyrelserna

Polisen