Information on

Money laundering and terrorist financing

for providers of **money transfer services**

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

The following information is intended for payment institutions and registered payment service providers that offer the service money transfer services. Because you provide money transfer services, there is a significant risk that you will be exposed to money laundering and terrorist financing. The purpose of this brochure is to increase your awareness of these crimes.

Here you will find information about the methods that are used for money laundering and terrorist financing, as well as the various risks that may be associated with your area of business. We also describe certain situations and red flags that may indicate that your business is being used to launder money or finance terrorism. You will also get an overview of your obligations under Sweden's anti-money laundering regulations.

This information is provided by the Coordinating Body for Anti-Money Laundering and Countering Financing of Terrorism. This information has been produced by the Swedish Financial Supervisory Authority, the Financial Intelligence Unit and the Swedish Security Service.

The Coordinating Body consists of 17 members and is led by the Swedish Police Authority. It serves as a forum for information exchange and knowledge transfer. The Coordinating Body's assignment is to identify, map and analyse risks and methods for money laundering and terrorist financing in Sweden and provide information for operators within Sweden.

On the Swedish Police's website **polisen.se/penningtvatt**, you can find more information on money laundering and terrorist financing as well as information about the Coordinating Body.

Published by: The Swedish Police Authority:
Registration number: A634.005/2021
Version: December 2021
Graphic form: Blomquist Communication, blomquist.se
Photo: Shutterstock

Your business is at risk of being exploited

Don't risk participating in crime! Because you provide money transfer services, you are obliged to prevent the risk that your business will be used as a tool for criminal activity. You can ensure doing this by following the anti-money laundering regulations.

Criminal actors in Sweden use cash to make it more difficult to trace money and reduce the risk of detection. Since banks in Sweden have reduced the degree to which they handle cash, criminals are turning to other channels to carry out their illegal cash transactions. In a money transfer, money can be sent without opening a payment account in either the payer's name or the recipient's name. It is a channel that criminals use in money laundering schemes to conceal the connection between the funds and criminal activity, or when money is sent with the intention of financing terrorism. The combination of a high proportion of cash in the money transfer business and the prevalence of cross-border transactions means that the risk that the business will be used for these activities increases.

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 financial support of terrorism by collecting, providing or receiving money or other property that is intended to finance terrorism.

In terrorist financing schemes, so-called reverse money laundering is common, which means that instead of laundering criminal profits, legitimately earned money is often used for illegal activities. This does not rule out the possibility that the money comes from criminal activities, but the main goal of a terrorist financing scheme is to conceal the money transfer until it reaches its final destination.

Regulations

Because you provide money transfer services, you are obliged to follow

- the Anti-Money Laundering and the Financing of Terrorism (Prevention) Act (2017:630), shortened to the Anti-Money Laundering Act,
- the Swedish Financial Supervisory Authority's regulations (FFFS 2017:11) regarding measures against money laundering and terrorist financing, and
- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

Any person who who wishes to provide money transfer services must receive authorisation from the Swedish Financial Supervisory Authority. Any person who conducts payment transfers with a turnover exceeding the equivalent of EUR 3 million per month must have authorisation to conduct payment service operations and is referred to in the Payment Services Directive as a payment institution. Persons with a lower turnover can apply for an exemption from the authorisation obligation and are referred to as registered payment service providers.

Hawala
Hawala refers to a financial service that is carried out outside an established financial system. In practice, this can be a scenario where the sender and receiver physically move money between themselves, as it is not technically possible to settle the transaction (i.e., perform clearing) in any other way. It may also be the case that receivables are cleared between sender and receiver without funds ever being transferred.

In order to provide hawala services, authorisation is required from the Swedish Financial Supervisory Authority in accordance with the Payment Services Act. In order to be granted authorisation, the business must meet the requirements for this type of service and be in compliance with Swedish anti-money laundering regulations.

Your obligations under Swedish anti-money laundering regulations

Money laundering regulations are often referred to as risk-based regulations. The regulations impose requirements on you as an operator to be informed of the risks of money laundering and terrorist financing. This also means that you must be able to work to address these risks in your business. If you provide money transfer and other payment services through an agent, you are responsible for ensuring that the agent meets the requirements under Swedish money laundering regulations.

Taking a risk-based approach means, in part, that you need to take risk-based measures to prevent your business from being used for money laundering and terrorist financing. The measures you need to take will depend on the risks you are exposed to. As stated above, it is your responsibility to to be aware of and analyse these risks.

General risk assessment

Because you provide money transfer services, you are obliged to perform a general risk assessment. This means that you need to assess how the products and services you provide in your business can potentially be used for money laundering and terrorist financing and the magnitude of the risk of this occuring. You must pay special attention in your assessment to your products and services, your customers and distribution channels, and the geographical risk factors in your business.

You must also consider relevant information provided by the authorities. This may include risks presented in publications from law enforcement agencies and the Swedish Financial Supervisory Authority. If your activities as a provider of money transfer services include business conducted through one or more agents, you must also specify in your general risk assessment the the risks associated with the agents' activities; for example, the agents may be located in an area that the Swedish Police Authority defines as a vulnerable area.

The general risk assessment must be adapted to account for the size and nature of your business as well as the inherent risks. The assessment must be documented and kept up to date. The general risk assessment must constitute the basis for your routines and guidelines as well as other measures that you take to prevent your business from being used for money laundering and terrorist financing.

Routines and guidelines

Because you provide money transfer services, you must have established routines and guidelines in place for, among other things, customer due diligence, monitoring and reporting. The purpose of these routines and guidelines is to counteract the risks that you identified in the general risk assessment. It is therefore important that you adapt your routines and guidelines according to the general risk assessment.

Risk assessment of customers

In addition to performing a general assessment of the risks associated with your own business, you need to assess the risk of money laundering and terrorist financing in relation to each individual customer, i.e. the customer's own risk profile. When you perform a risk assessment of your customers, you should start from the general risk assessment you performed for your own business and the information you have about each customer. It is important that you follow up on each customer's risk profile and, if necessary, adjust the risk levels.

Customer due diligence – do you know who your customer is?

Because you provide money transfer services, you need to perform adequate customer due diligence measures, that is, you must be well informed of who your customers are. This means that when you establish a new business relationship, you must take customer due diligence measures to learn who your customer is. This entails verifying your customers identity and checking whether a customer is someone in a politically exposed position. You also need to include information about the purpose and nature of the business relationship, i.e., information about how the customer will use your products and services. The term business relationship refers to a customer relationship that is expected to be maintained over an extended period of time.

You also need to take customer due diligence measures for customers who carry out individual transactions amounting to the equivalent of EUR 1,000 or more. This also applies when several transactions can be assumed to be related and together amount to the equivalent of EUR 1,000 or more. If you do not have enough knowledge about the customer to manage the risk of money laundering or terrorist financing that may be associated with the customer relationship, or if you do not have adequate knowledge about the customer to enable you to monitor and assess the customer's activities and transactions, do not establish a customer relationship. If the person is already a customer, you must terminate the business relationship.

Monitoring and reporting

You must monitor ongoing business relationships and review individual transactions in order to detect suspicious transactions and other activities, as well as transactions and activities that deviate from what you already know about the customer and transactions that can be assumed to be part of a money laundering or terrorist financing scheme. Throughout the duration of the business relationship you must continuously monitor the customer's transactions and follow up on the business relationship. The extent of the monitoring that is required will depend on the customer's risk profile. Transactions and other activities performed by customers who have been assessed as high-risk, will need to be monitored and followed up on more thoroughly than those performed by low-risk customers.

If you have reasonable grounds to suspect a customer is involved in money laundering or terrorist financing, or that the customer's property originates from a criminal activity, you are obliged to report to the Financial Intelligence Unit without delay. The Financial Intelligence Unit is a unit within the Swedish Police Authority that receives, registers, processes and analyses reports of suspected money laundering or terrorist financing. In cases of suspected terrorism, the Financial Intelligence Unit immediately sends an intelligence file to the Swedish Security Service for assessment and investigation. If the Swedish Police Authority or the Swedish Security Service so request, you are also obliged to hand over without delay all information necessary for an investigation into money laundering or terrorist financing. You must have an established system so that you can provide such information quickly.

You are prohibited from establishing a business relationship or carrying out an individual transaction if you suspect that your products or services may be used for money laundering or terrorist financing. You may only carry out a suspicious transaction if it is impossible to refrain from doing so or if it would compromise the investigation if you did not carry out the transaction. In this case, you must immediately prepare a report after the transaction and submit it to the Financial Intelligence Unit.

Even if you decide not to carry out a transaction due to the suspicion of money laundering or terrorist financing, this must be reported to the

Financial Intelligence Unit. Your reporting obligation continues to apply even if the transaction is not completed or the business relationship is terminated.

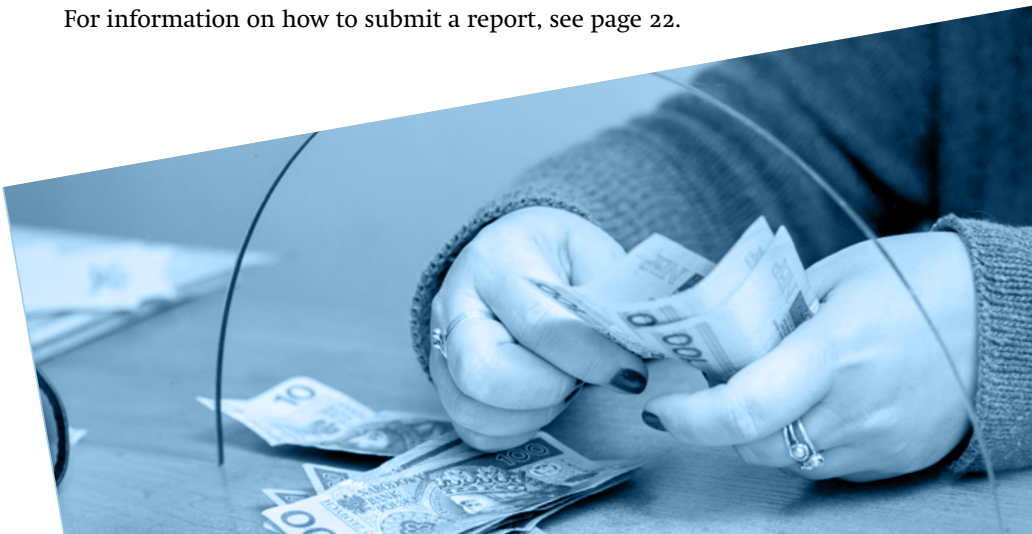
A report to the Financial Intelligence Unit is not the same as a police report. Information about who submitted the report and what has been reported is kept secret.

You have a confidentiality obligation, but this does not apply in your relationship with the Swedish Financial Supervisory Authority.

In this context, you are subject to the confidentiality obligation. This means that you may not inform the customer or any outside party that a more detailed review has taken place or that a report of suspected money laundering or terrorist financing has been submitted to the Financial Intelligence Unit. On the other hand, you do not violate your confidentiality obligation by providing information to the Swedish Financial Supervisory Authority.

> Making a report to the Financial Intelligence Unit does not require that you, as a provider of money transfer services, have evidence that money laundering or terrorist financing has in fact taken place. It is enough that you have reasonable grounds to suspect that such a crime has taken place or that, for example, the funds originate from criminal activity.

For information on how to submit a report, see page 22.



Suitability assessment routines

You must have procedures in place to ensure the suitability of employees, contractors and others involved in your business, if their work duties are significant in preventing the business from being used for money laundering or terrorist financing. These procedures must ensure that these individuals are informed about money laundering and terrorist financing at a level that is appropriate for their work duties and functions. The established procedures must also contain a description of how you as a provider of money transfer services otherwise ensure that an individual is suitable for the work tasks he or she is expected to perform.

Training

You must ensure that employees, contractors and others involved in your business who perform tasks that are significant in preventing the business from being used for money laundering or terrorist financing receive ongoing training and up-to-date information. This measure fulfills in part your obligations under the Anti-Money Laundering Act. At a minimum, training must include the relevant parts of money laundering regulations, your general risk assessment, your routines and guidelines and information that facilitates the detection of suspected money laundering and terrorist financing.

Other regulatory provisions

The Anti-Money Laundering Act and other anti-money laundering regulations contain additional provisions that you are obliged to follow as a provider of money transfer services, including provisions on the processing of personal data, internal controls and data documentation.

Intervention

If you, as a provider of money transfer services, fail to fulfil your obligations under anti-money laundering regulations, the Swedish Financial Supervisory Authority may intervene in certain cases. As a result of the authority's intervention, you may be required, for example, to take corrective measures to remedy deficiencies, pay a sanction fee or cease operations, i.e., terminate business activities. The form of intervention the authority takes depends, among other things, on how serious the violation is and the type of authorisation you have from the Swedish Financial Supervisory Authority.

Source: Payment Services Act (2010:751)

Information about penalties for money laundering
Possessing or dealing with property arising from a crime or criminal activity constitutes money laundering if the actions are taken with the aim of concealing the illicit origin of the property or to facilitate the opportunity of a third party to enjoy the property. If, in the course of your business activities, you participate in an action that can reasonably be assumed to have been taken for the purpose of concealing the illicit origin of money or other property or to facilitate the opportunity of a third party to enjoy this money or property, you can be convicted of commercial money laundering.

Any person who engages in money laundering or commercial money laundering may be convicted of a crime and sentenced to prison. The decisive factor for a money laundering conviction is not that the money originates from critical activities. You can be convicted of commercial money laundering even if the property originates from legitimate activities. The criteria for criminal liability is instead that you are guilty of culpable risk-taking.

Any person convicted of money laundering may also be liable for damages, or the money/property may be seized in accordance with the Act on Penalties for Money Laundering Offences (2014:307). Any convicted of money laundering may have their property taken into custody in accordance with the Act on Certain Stolen Goods etc. (1974:1065)

Source: Act on Penalties for Money Laundering Offences (2014:307).

Examples of risks and approaches

Below are examples of situations that you and your agents need to be aware of. This is especially true when multiple red flags occur simultaneously or repeatedly, but this also applies if only one red flag occurs. This does not have to mean that something illegal has in fact occurred, just that you as a provider of money transfer services or your agents may need to perform a more thorough review of the transactions and your customers.

Cash handling

All cash handling, especially in larger amounts, entails a higher risk of money laundering. The use of cash is generally declining in Sweden, and cash is largely being replaced by card payments and electronic payment services, such as Swish. But at the same time, cash continues to be important for criminals because criminal activities can generate large amounts of cash. This cash may be illicit profits from the drug and weapons trade, trafficking or money obtained from international theft and receiving networks.

Dummy owners and straw men

It may be the case that a sender or recipient is acting as a dummy owner or straw man for criminal actors, or that a sender or recipient is using false identity documents. This often indicates that someone is attempting to conceal their own or someone else's identity and that the money being transferred comes from criminal activities. It is therefore important to perform thorough checks to verify the customer's identity and take customer due diligence measures when needed.

If the customer cannot satisfactorily explain the origin of the money or the purpose of the transaction, this should arouse suspicion. The same applies if the amount to be transferred differs based on what is known about the customer's financial situation or is unusual in some other way that cannot be explained by the customer. If a customer wishes to make a transaction with another person's credit card, this can also be a cause for suspicion.

Avoidance of checks

Anti-money laundering regulations require, among other things, that money transfer transactions be subject to customer due diligence measures, if the amount exceeds EUR 1,000. As a provider of money transfer services, you should therefore take note of whether a customer is trying to avoid customer due diligence measures by sending several transactions that are just under EUR 1,000. For example, several people may come to your business wishing to send such amounts to the same recipient. In such situations, these transactions might constitute money laundering. The money might also originate from fund-raising activities with the intention of financing terrorism.

If, as an agent, you provide money transfer services via more than one payment system, it should arouse suspicion if a customer wishes to send money through several different systems at the same time. This is especially true if the recipient of the money is the same person.

The relationship between sender and receiver

If you do not understand the relationship between a sender and a recipient, a transaction between these parties can be considered suspicious. In addition, if the recipient is in a country where the risk of money laundering or terrorist financing is assessed to be high, a so-called high-risk country, or in an area in another country that borders a high-risk country, there is cause to take extra precautions and ask more questions about the purpose of the transaction. You are responsible for assessing which countries can be considered high-risk countries for your business.

Money transfers without a clear purpose

Transactions where both the sender and recipient are in Sweden can also be grounds for suspicion of money laundering. This is especially true if someone is sending money to a person who is nearby geographically.

If you become aware that a customer is carrying out several transactions through several different agents without a reasonable explanation, this may also be considered suspicious behaviour.

Other payment services that can be used for money laundering

Agents sometimes offer payment services other than money transfer. For example, agents may offer clients the option to deposit cash in bank accounts, settle accounts or make cash withdrawals by card payment. There is a risk that these services may also be used for money laundering. For example, illicitly obtained cash can be paid in to bank accounts or through bankgirot and postgiro and then integrated into the financial systems to conceal the origin of the money. If cash is withdrawn, there is a risk that it will be used, for example, to pay illegal wages or in other criminal activities.

Financing of terrorism

Providers of money transfer services for illegal purposes purposes by transferring money from Sweden to terrorist organisations abroad. Money transfer services are easily accessible and offered by a large number of agents with an extensive geographical distribution around the world. This business area can therefore be used as a channel for what can be suspected to be terrorist financing. These transactions can be significant links in the chain to bring money out of Sweden to high-risk countries and conflict zones.

As cash transactions are common in the money transfer business, it is difficult for authorities to trace the transaction chains. Recipients are largely able to remain anonymous, as it is not possible to verify the identity of the person who collects the money, and in the context of terrorist financing, it is the recipient that is the crucial party.

Actors do not need access to a large amount of capital to finance, plan, prepare and execute a terrorist attack. This means that it is crucial to prevent even small amounts of money from reaching the intended recipient, as this helps to reduce the risk of terrorism and weakens the financial capacity and operations of terrorist organisations. When it is a question of terrorist financing, it is the entended use of the money that is crucial. There is no need for a series of predicate offences, and many terrorist crimes have been financed with relatively small amounts of money that have been legally obtained. Terrorist financing refers not only to the financing of terrorist attacks but also the financing of recruitment and training efforts of a person or an organisation that intends to commit terrorist acts.

Hawala

Informal payment systems, sometimes called hawala, can be used for money laundering and terrorist financing. This is because hawala creates an opportunity for actors to carry out transactions anonymously and to send money to conflict zones. Hawala also makes it possible to transfer money to jurisdictions that are subject to sanctions and do not have agents for the larger payment institutions, as well as to war zones with a lack of technical infrastructure.

Facts about penalties for the financing of terrorism

In certain cases, it is prohibited to collect, provide, or receive money or other property. This is the case when the purpose of the property is to support terrorist activities or when an individual is aware 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.

Source: Act on Criminal Responsibility for the Financing of Particularly Serious Crimes, in some cases (2002:444).

Be vigilant!

1 Red flags linked to customer behaviour

- The customer is nervous, stressed or acts in a threatening manner.
- You suspect that the customer is sending money on behalf of someone else. For example, you notice people waiting outside when the transaction is being completed.
- The customer is a minor.
- The customer refers to lists or what appear to be instructions (on paper or digitally) to keep track of different currencies and amounts.
- The customer shows an unusual amount of interest in your business's routines.

2 Red flags linked to the customer's identity

- The customer is unable to verify his or her identify upon request.
- The customer presents identity documents that are suspect, for example, damaged documents.
- The customer is domiciled (is a resident) in a country that the EU Commission has identified as a high-risk third country.
- The customer presents different identity documents on different occasions.
- The customer is unable to present any documents that identify the company the customer represents.

3 Red flags linked to the customer's transactions

- The customer wishes to transfer large sums of cash.
- The customer regularly sends money without an obvious reason to do so.
- The customer changes his or her behaviour pattern and suddenly starts sending amounts or currencies that differ from previous transfers.
- The customer is indifferent to fees and exchange rates and sends small sums despite fees.
- The customer wishes to send money in a way that cannot be explained based on what is known about the customer's financial position.
- The customer wishes to send money to recipients to whom the customer has no natural connection.
- The customer wishes to send money to many different recipients, who may reside in different places.
- The recipient or recipients of the transactions have previously received suspicious transactions.

4 Red flags linked to the customer's responses to questions

- The customer refuses to answer questions about the origin of the money or the purpose of the money transfer.
- The customer terminates the transaction when you ask questions.
- The customer lacks documentation or presents documentation that cannot be verified.
- The customer states the same purpose for multiple transfers on several occasions.
- The customer wishes to transfer money to conflict areas but lacks a reasonable explanation for why.
- The customer tries to avoid questions by offering an explanation or documentation before you have requested it.
- The customer does not seem to have enough information about the purpose of the transfer.
- The customer states that the money is being sent to relatives but sends money to many different people in different places, and the names of the recipients do not indicate that they are in fact relatives.

How to report

In order 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. This can take up to two working days. It is therefore recommended 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.

The Financial Intelligence Unit's website (see address below) contains manuals for registration and reporting in goAML as well as other material you will need to get started.

goAML's website: **https://fipogoaml.polisen.se**

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.

Sweden's anti-money laundering regulations are updated continuously. In case of discrepancies between the contents of this brochure and the wording of anti-money laundering regulations, the wording in the regulations shall take precedence.

More information

More information about money laundering and terrorist financing, as well as rules for money transfer services, can be found on the Swedish Financial Supervisory Authority's website: www.fi.se.

If you have any questions about anti-money laundering regulations or this brochure, please contact:

The Swedish Financial Supervisory Authority
Switchboard: 08-408 980 00
Email: finansinspektionen@fi.se

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

FINANSINSPEKTIONEN

Polisen