Information to **currency exchangers** about

Money laundering and terrorism financing

THE COORDINATING BODY FOR AML/CFT

This folder is designed to provide you, as a currency exchanger, with information about money laundering and terrorism financing. It explains the risks that are linked to your enterprise.

We are providing this information to give you and other currency exchangers a better understanding of how money laundering and terrorism financing is carried out. We describe various scenarios and warning signals that can indicate that you as a currency exchanger is being used to launder money or finance terrorism. We also summarise your obligations as a currency exchanger according to the money laundering regulations.

This information has been produced by The Coordinating Body for Anti-Money Laundering and Countering Financing of Terrorism in consultation with Sweden's Financial Supervisory Authority (Finansinspektionen).

The Coordinating Body has 17 members and is headed by the Swedish Police. It is a forum for information exchange and knowledge transfer, and it is tasked with identifying, surveying and analysing risks of and methods for money laundering and terrorism financing in Sweden.

Representatives in the Coordinating Body

Swedish Companies Registration Office
Swedish National Council for Crime Prevention
Swedish Economic Crime Authority
Swedish Estate Agents Inspectorate
Swedish Financial Supervisory Authority
Swedish Enforcement Authority
County Administrative Board of Skåne
County Administrative Board of Stockholm
County Administrative Board of Västra Götaland
Swedish Police Authority
Swedish Inspectorate of Auditors
Swedish Gambling Authority
Swedish Tax Agency
Swedish Bar Association
Swedish Security Service
Swedish Customs
Swedish Prosecution Authority

For more information, please visit the Swedish Police web site: www.polisen.se/penningtvatt

Publisher: Swedish Police Authority
Registration number: A363.983/2020
Version: July 2020
Graphic design: Sinfo Yra

Your enterprise is at risk

Do not risk contributing to criminal activities. As a currency exchanger, you are responsible for preventing the possibility that your enterprise can be used for criminal activity. You do this by complying with the Anti-Money Laundering and Countering Terrorism Financing Act (2017:630).

In Sweden, it is common for criminals to use cash since it is harder to trace and reduces the risk of discovery. As banks in Sweden have reduced the amount of cash they handle, criminals have begun to use other business for this, such as currency exchangers and money transfer businesses.

If a customer exchanges many smaller denomination banknotes for larger ones, this could suggest some kind of collection activity to finance terrorism. If a customer exchanges larger denomination banknotes, this could be a sign of courier activity, i.e. that large sums of cash are being moved across country borders to finance terrorism.

Similarly, people who want to support terrorism use currency exchangers to exchange Swedish kronor for a currency that is used in areas where terrorist-organisations are active.

Money laundering means that dirty (illegal) money is laundered to make it look as if it has been earned legally. The aim is to use the money from criminal activities in the legal economy. For example, the money in question might be proceeds from drug-related crimes or frauds.

Terrorism financing means financially supporting terrorism and collecting, providing or receiving money or other assets to be used in the financing of terrorism.

The Regulatory Framework

As a currency exchanger, you are responsible for complying with:

- Anti-Money Laundering and Countering Terrorism Financing Act (2017:630) (the Anti-Money Laundering Act), and
- Finansinspektionen's regulations (FFFS 2017:11) regarding measures against money laundering and terrorist financing.

Your obligations under the Anti-Money Laundering Act

The Anti-Money Laundering Act requires you as a currency exchanger to take so-called risk-based measures to prevent your enterprise from being used for money laundering and the financing of terrorism. The measures you should take depend on the risks that you believe your enterprise is exposed to.

General risk assessment

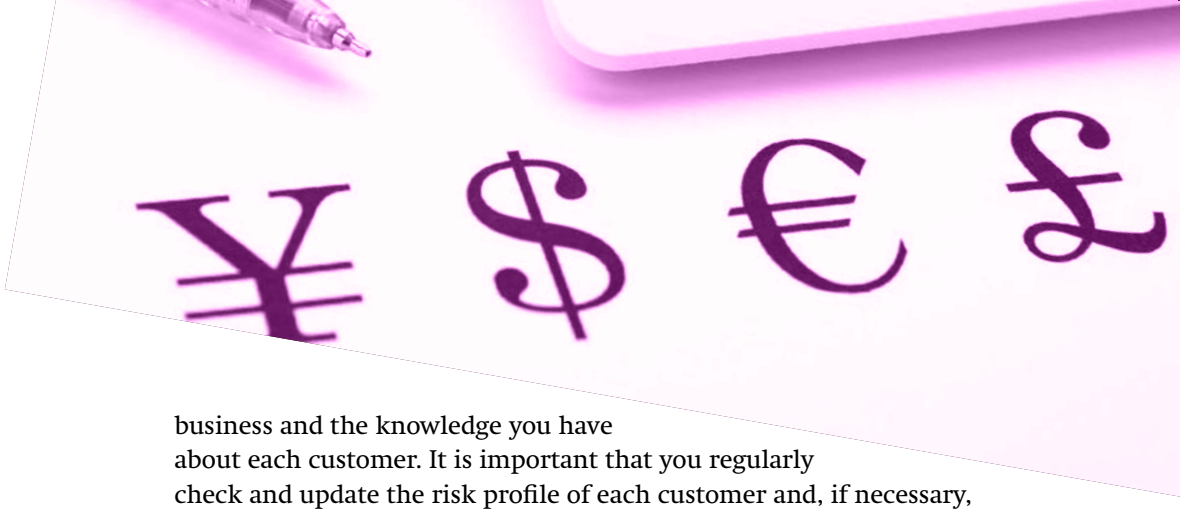
How can the products and services that you offer in your business be used to launder money or finance terrorism? How big is the risk that this could happen? As a currency exchanger, you should conduct a general risk assessment. You should document the assessment and update it regularly. Your general risk assessment should form the basis for the procedures and other measures that you use to prevent your enterprise from being used for money laundering and terrorism financing.

Procedures

As a currency exchanger, you should have internal procedures in place for e.g. knowledge about your customers, supervision and reporting. Such procedures are designed to counter the risks you have identified in your general risk assessment. It is therefore important that these procedures are adapted to the general risk assessment.

Risk assessment of customers

In addition to conducting a general assessment of the risks in your enterprise, you should also assess the risk of money laundering and the financing of terrorism that each customer can be associated with; in other words, create a risk profile for each customer. Risk assessments of customers should be based on your general risk assessment of your



business and the knowledge you have about each customer. It is important that you regularly check and update the risk profile of each customer and, if necessary, change their risk level.

Know your customers – who are they?

As a currency exchanger, you should know your customers, that is to say, you should be as aware as possible of who your customers are. When your enterprise establishes a new business connection, you should take steps to learn more about the customer. This means finding out who the customer is. For example, you should be able to identify your customers and check if a customer has a politically exposed position. You should also obtain information about the purpose and nature of the business connection. Here, a business connection means a customer relationship that, once established, can be extended and continue for a longer period. You should also get to know customers that engage in individual transactions for €15,000 or more. You should also learn more about customers who engage in multiple transactions that can be assumed to be related to one another and together total €15,000 or more.

If you do not know enough about a customer to be able to manage the risk of money laundering or the financing of terrorism that can be associated with the customer relationship, or if you do not know enough about the customer to be able to monitor and assess the customer's activities and transactions, you should not do business with the customer. If the person is already a customer, you should end the business connection.

Monitoring and reporting

As a currency exchanger, you should monitor ongoing customer relationships to detect activities or transactions that are suspicious or

seem not to fit with what you know about the customer. During the entire time a person is a customer, you should monitor their transactions and the business connection on an ongoing basis. How much monitoring you will need to do will depend on the risk profile of the customer. In other words, any transactions and other activities carried out by customers you consider to have a high risk must be monitored and evaluated more carefully than those carried out by low-risk customers.

If you suspect money laundering or the financing of terrorism, you should report this to the Swedish Financial Intelligence Unit immediately. You must not delay such reporting. As a currency exchanger, you may not tell the customer or any other external party that you have reviewed the transactions or that you have sent a report to the Swedish Financial Intelligence Unit. For more information on reporting, please see page 13.

Other requirements

The Anti-Money Laundering Act contains several other requirements that you as a currency exchanger must comply with, such as the processing of personal data, training of personnel and documentation of data.

Penalties for money laundering offences

If you as a currency exchanger are involved in any actions that can be assumed to have been taken to conceal the fact that money or other property comes from criminal activity or help someone to profit from such money/property, there is a risk that you could be convicted of an offence under the Money Laundering Offences Act.

You do not have to have been aware that the money originated from criminal activity; it is enough that you should have realised it. This means that if you do not fulfil the requirements in the Anti-Money Laundering Act there is a risk that you could be sentenced to fines or imprisonment for engaging in, for example, money laundering activities.

Source: Money Laundering Offences Act (2014:307)

Methods

Large sums and large denomination banknotes

Generally speaking, cash is used less in Sweden. Cash is being replaced largely by card payments and electronic payment services, such as Swish. At the same time, cash continues to be important for criminals as criminal activities often generate large sums in cash. This can be profits from illegal drugs and arms dealing, trafficking or money from international theft and handling of stolen goods. Any time a large amount of cash is processed, there is a high risk that it is connected to money laundering. Within certain types of criminality, such as smuggling, large sums are transported in cash abroad to pay for deliveries or to export profits. This is often done after Swedish money has been exchanged for larger denominations in foreign currencies, such as euro and dollars.

Middlemen and repeat exchange transactions

Criminals often use intermediaries when they exchange money. As a currency exchanger, you should therefore pay particular attention if very young individuals or individuals who would seem to have limited financial resources process large sums. This could suggest that these individuals are being used as intermediaries for criminals. Also pay close attention to people who repeatedly exchange money, as it is unusual to need to exchange money on a regular basis. Multiple exchange transactions could also accumulate to large amounts relatively quickly, which is high-risk activity.

Exchanging denominations in the same currency

Customers who wish to exchange denominations in the same currency, such as Swedish banknotes in smaller denominations for Swedish banknotes in larger denominations, are associated with a high risk. Enterprises normally process cash via a company or a bank. There is therefore a high risk that this money comes from criminal activity or a black-market business that generates cash.

Cash couriers and the financing of terrorism

Money laundering and terrorism financing are similar but also different. The biggest difference is that money laundering aims to conceal the origin of the money while terrorism financing aims to conceal what the money is going to be used for. In the case of the financing of terrorism, so-called reverse money laundering is common practice. Instead of laundering the proceeds of crime, legally acquired money is often used for illegal activities. This does not exclude the possibility of the money originating from crime, but when financing terrorism, the main aim is to conceal the movement of the money to the final destination.

Recent international research shows that some of the most common ways of moving financial assets to finance terrorism are via cash couriers and informal transfer systems such as hawala, but that payment service providers, bank transactions, false invoices and precious metals are also used.

If a customer wishes to exchange many small denomination notes for larger ones, this can suggest some kind of collection activity with the aim of financing terrorism. Larger denominations are also easier for couriers smuggling currency to handle.

Be on your guard

The following examples of warning signals can give you as a currency exchange, a reason to perform a more detailed audit of the customer and the customer's transactions. This is especially the case if several warning signals occur at the same time or repeatedly. The warning signals are not definite signs of illegal activity, but rather simply help you as a currency exchanger to know that you need to take a closer look.

1 Warning signals linked to customer behaviour

- The customer appears to be nervous, stressed or threatening.
- The customer appears to be exchanging money on behalf of someone else. For example, individuals might be waiting outside during the transaction.
- The customer is a minor or is known to be a substance abuser.
- The customer is following lists or what appears to be instructions (on paper or on a digital device) to keep track of different currencies and amounts.
- The customer expresses an exaggerated interest in currency exchange procedures.

2 Warning signals linked to customer identity

- The customer cannot provide ID on request.
- The customer presents ID documentation that looks odd, for example it is damaged.
- The customer is from a country that the European Commission has identified as a high-risk third country outside the EEA.
- The customer presents different ID documents on different occasions.
- The customer cannot show any documentation identifying the enterprise they represent.

3 Warning signals linked to customer transactions

- The customer wishes to exchange large sums in cash.
- The customer wishes to exchange banknotes of the same currency, such as Swedish kronor, to different denominations of Swedish kronor.
- The customer makes regular exchange transactions for no apparent purpose.
- The customer changes their behaviour pattern and suddenly starts to exchange amounts or currencies that do not correspond with previous exchange patterns.
- The customer is not bothered about charges and exchange rates, and exchanges small sums despite the charges.
- The customer wishes to exchange money in a way that cannot be explained based on what is known about the customer's financial circumstances.
- The customer wishes to obtain a currency to which the customer does not have any natural connection.

4 Warning signals linked to customer answers to questions

- The customer does not wish to answer questions about the origins of the money or the reason for the exchange.
- The customer terminates the transaction when asked questions.
- The customer lacks supporting data or presents data that cannot be checked.
- The customer states the same purpose for the exchange on several occasions.
- The customer states that they are going to travel to conflict areas.
- The customer tries to avoid questions by offering an explanation or supporting data before being asked by the currency exchanger.
- The customer does not appear to be sufficiently aware of the reason for the exchange.

You are required to report suspicious transactions and activities

As a currency exchanger, you are required to report suspicious transactions and activities.

Even if you suspect money laundering or terrorism financing and choose not to carry out the transaction, you must still report the transaction to the Swedish Financial Intelligence Unit. Your obligation to report the transaction does not disappear just because you did not carry out the transaction or ended the business connection.

Currency exchangers are not required to have hard evidence that money laundering or terrorism financing has taken place before reporting to the Swedish Financial Intelligence Unit. It is enough that you reasonably suspect that this is the case or, for example, that the money comes from criminal activities.

Reporting to the Swedish Financial Intelligence Unit is not the same as reporting to the Police. The details of who has submitted the report and what has been reported remain confidential.

Transactions and reports are confidential

In this context, currency exchangers are subject to an obligation of confidentiality. Obligation of confidentiality means that you as a currency exchanger must not tell the customer or any other external party that you have reviewed their transactions in detail or sent a report of suspected money laundering or terrorism financing to the Swedish Financial Intelligence Unit. However, you are allowed to submit information to Finansinspektionen without violating this obligation.

How to submit a report

You can submit a report to the Swedish Financial Intelligence Unit via the IT system goAML.

In order to be able to access the online portal and submit reports about suspicious transactions and other activities, you will need to register your enterprise and create a user account.
The address for goAML is
https://fipogoaml.polisen.se

There is a manual in the portal that explains how you can register your enterprise and create user accounts in goAML. If the details you entered are correct, the Swedish Financial Intelligence Unit will confirm your registration within two working days. Once you receive your confirmation, you can log in to the portal. There is a manual about reporting and other materials to help you get started.

The address for goAML is
https://fipogoaml.polisen.se

Questions about goAML

You will find most answers in the manuals and other material that you can access after registering. If you cannot find the answer to your question in the manuals or other material, please email fipo@polisen.se.

In the event that the information contained in this brochure is different from the regulatory requirements, the regulatory requirements will always take precedence.

More information

More information on money laundering, terrorism financing and rules for currency exchangers is available at Finansinspektionen's website: www.fi.se.

THE COORDINATING BODY FOR AML/CFT

FINANSINSPEKTIONEN

Polisen
Swedish Police