

---

## 9. Vulnerability of the dealers' sector

---

### 9.1. General description of the sector

In accordance with § 2 1) of the Trading Act, “dealer” means a person or body which, within the framework of the economic or professional activities thereof, offers and sells goods or offers and provides services. In accordance with § 2 (1) 5) of the Money Laundering and Terrorist Financing Prevention Act (MLTFPA), the Act applies to dealers where a cash payment of no less than EUR 10,000 or an equivalent sum in another currency is made to or by the dealer, regardless of whether the financial obligation is performed in the transaction in a lump sum or by way of several linked payments over a period of up to one year, unless otherwise provided by law. Additionally, persons engaged in buying-in or wholesale of precious metals, precious metal articles, or precious stones are considered to be dealers within the meaning of this report. If a person engages in buying-in or wholesale of precious metals and/or precious metal articles used for production, scientific and/or medical purposes, the MLTFPA is not applied to the person unless they fall under another criteria specified by § 2 of the MLTFPA.

Compared to the previous risk assessment, the scope of application of law in relation to dealers has been expanded. Until 27 November 2017, the limit of cash payment from which a dealer became an obliged entity was EUR 15,000. The change came from the European Union law. In the recitals of the Anti-Money Laundering Directive IV, large cash transactions were considered so unusual that it was decided to establish a lower threshold. Several member states have adopted even lower thresholds at the national level. In accordance with recital 6 of the Anti-Money Laundering Directive IV, in order to increase vigilance and mitigate the risks posed by such cash payments, persons trading in goods should be covered by this Directive to the extent that they make or receive cash payments of EUR 10,000 or more. The member states should be able to adopt lower thresholds, general additional restrictions to the use of cash, and additional stricter provisions.

Usually there is no authorisation procedure applied to dealers for trading (except for a few exceptions such as sale of alcohol). Additionally, no specific type of legal entity is required to engage in dealing. A dealer may be any person who, in the course of their economic or professional activities, offers and sells goods or services. Therefore, dealers do not constitute a delimited group of persons like credit institutions or sworn auditors. As becoming an obliged entity depends on activities as well as payment methods and payment amounts, the necessary subsectors for constructing the sample for the analysis were chosen based on the probability of large-scale cash payments. The choice of subsectors was influenced, for example, by the prevalence of high-priced services or goods in the subsector or the popularity of cash in the subsector.

It was also taken into consideration that the persons who are obliged entities within the meaning of the MLTFPA on a basis other than § 2 (1) 5) of the MLTFPA belong to another sample than the dealers in this analysis, as they did not become obliged entities due to circumstances arising from a transaction but in relation with their field of activity. An exceptional addition to the dealers' sample is the dealers of precious metals, precious metal articles, and precious stones specified in § 2 (1) 6) of the MLTFPA. In order to define the sample, Estonian Classification of Economic Activities (CEA codes) was used. Companies operating under a total of 29 different CEA codes were included in the dealers' sector.

**Table 49.** Overview of the dealers' sector

Group of sectors	Subsector	Number of companies
Construction	Renting and leasing of construction and civil engineering machinery and equipment	371
	Construction of residential and non-residential buildings	8274
	Retail sale of other building material and goods in specialised stores	135
	Retail sale of furniture and articles for lighting in specialised stores	220

<b>Vehicles</b>	Sale of cars and light motor vehicles (with a weight not exceeding 3.5 tons)	1234
	Sale of other motor vehicles	286
	Maintenance and repair of motor vehicles	2165
	Retail trade of motor vehicle parts and accessories	833
	Renting and leasing of cars and light motor vehicles (with a weight not exceeding 3.5 tons)	875
	Renting and leasing of trucks	188
<b>Precious metals</b>	Wholesale of watches and jewellery	60
	Wholesale of metals and metal ores	217
<b>Retail sale</b>	Retail sale in non-specialised stores with food, beverages, or tobacco predominating	548
	Other retail sale in non-specialised stores	1324
<b>Luxury goods</b>	Retail sale of watches and jewellery in specialised stores	147
	Retail sale of souvenirs and craftwork articles in specialised stores	209
	Retail sale of antiques in stores	49
	Wholesale of alcoholic beverages	234
<b>Catering</b>	Restaurants, cafeterias, and other catering places	2905
<b>Real estate</b>	Buying and selling of own real estate	2561
	Renting and operating of own or leased real estate	9978
<b>Other transport</b>	Repair and maintenance of ships and boats	224
	Renting and leasing of water transport equipment	105
	Renting and leasing of air transport equipment	22
<b>Travel</b>	Travel agency activities	287
	Tour operator activities	236
<b>Health care</b>	Specialist medical practice activities	387
	Dental practice activities	535
<b>Beauty services</b>	Hairdressing and other beauty treatment	4746

Several umbrella organisations and professional associations operate within the sectors listed in the table above: Estonian Chamber of Commerce and Industry, Estonian E-Commerce Association, Estonian Traders Association, Estonian Vehicle Dealers and Services Association (AMTEL), and in the beauty sector, Estonian Beauticians Association and Estonian Hairdressers Association. Membership is not mandatory.

Hereinafter, when assessing the sample size on the basis of CEA codes, only the companies that have submitted their annual report during the observed period and indicated their main field of activity with the relevant CEA code, are included. However, it should be taken into account that the results obtained in this way show the magnitude rather than the exact number as those companies which are operating within this field as part of their additional activities, those which have mistakenly assigned a wrong CEA code, and those which for some reason have not submitted their annual report, are excluded. The sample included a total of 39,355 companies. Highest turnovers in years 2017-2019 were recorded in the sale of cars and light motor vehicles, retail sale in food stores, and construction and sale of real estate. It is not possible to unambiguously estimate the size of this sector on the basis of statistical indicators – essentially, all dealers within the meaning of the Trading Act are included at the moment when they make a large-sum cash transaction. Generally, the Financial Intelligence Unit (FIU) has expressed its opinion that large-sum cash transactions in Estonia are rather rare. Thus, not all persons in the sample are obliged entities according to the MLTFPA. For the purpose of the survey, dealers were again divided into the following groups: construction, vehicles, precious metals, retail sale, luxury goods, catering, real estate, other transport, travel, health care, and beauty services. Compared to the National Risk Assessment of 2015 (NRA 2015), the selection of the fields of activities in the dealers' sector has been expanded. New additions include construction, catering, real estate, travel, health care, and beauty services.

The largest exception in the dealers' sector is formed by persons engaged in buying-in or wholesale of precious metals, precious metal articles, or precious stones, as they are obliged entities due to their field of activity pursuant to the MLTFPA. When defining the field of activity, the following definitions of precious metals, precious metal articles, and precious stones provided by §§ 3 6)-8) of the MLTFPA are relevant:

- **Precious stones** – natural and artificial precious stones and semi-precious stones, their powder and dust, and natural and cultivated pearls
- **Precious metal** – pure gold, silver, platinum and palladium and their alloys
- **Precious metal article** – an object which is wholly or partially manufactured from one or several precious metals with at least the minimum standard of fineness permitted in §§ 4 (2) and (2<sup>1</sup>) of the Precious Metal Articles Act

The definition of precious stones in the MLTFPA uses precious stones as a generic concept with added specific concepts. Semi-precious stones, powder and dust of precious and semi-precious stones, and pearls also fall under the definition of precious stones in accordance with the MLTFPA. In accordance with § 70 (1) 6) of the MLTFPA, buying-in or wholesale of precious metals, precious metal articles or precious stones, except for precious metals and precious metal articles used for production, scientific or medical purposes requires an activity licence, unless any circumstances of clause 2 of the same section are present. This activity licence is issued to them by the FIU. It is difficult to assess the size of this subsector. According to the Register of Economic Activities, around 80 valid activity licences exist for buying-in and wholesale of precious metals and precious stones. However, the companies which have ceased activities are not erased from the Register of Economic Activities. Only those companies which are active, hold a valid activity licence, and whose main activity is related to precious metals, precious metal articles, or precious stones, were taken into consideration when defining the target group for the analysis.

**Table 50.** Data of the survey concluded in the dealers' sector

Subsector	Number of market participants	Sample size	Sample size / number of required responses	Number of invitations sent out	Number of responses received	Response rate
Construction: CEA code 41201, 77321, 47529, 47591	9000	sample	368	1620	475	129%
Vehicles: CEA code 45111, 45191, 45201, 45321, 77111, 77121	5581	sample	359	3348	982	274%
Precious metals: CEA code 46481, 46721	277	everyone	161	277	73	45%
Retail sales: CEA code 47111, 47191	1872	sample	319	1292	393	123%
Luxury goods: CEA code 46341, 47771, 477831, 47791	639	sample	240	638	215	90%
Catering: CEA code 56101	2905	sample	339	848	250	74%
Real estate: CEA code 68101, 68201	12529	sample	373	1760	503	135%

Other transport: CEA code 33151, 77341, 77351	351	sample	184	351	111	60%
Travel: CEA code 79111, 79121	523	sample	222	523	154	69%
Health care: CEA code 86221, 86231	922	sample	271	910	375	79%
Beauty services: CEA code 96021	4746	sample	355	888	281	79%

The participation activity in the dealers' sector survey has varied among different subsectors, but the overall participation of the dealers' sector in the conducted analysis is high. Therefore, the results of the survey were taken into account in the risk assessment.

## 9.2. Description of risk typologies

### **Cash transactions**

Cash constitutes the greatest risk in dealers' activities. § 2 of the MLTFPA has specified the cash threshold (above EUR 10,000) at which point dealers become the subject of law and are obliged to comply with the requirements of law and legal acts applied to an obliged entity, including applying due diligence measures and assessing risks related to their services, customers, and specific transactions. It became evident from surveys and working group discussions that many, predominantly smaller dealers comply with the abovementioned requirements insofar as to ensure the performance of the contractual obligations of the customer. This situation arises mostly due to low awareness of the dealers regarding the requirements related to money laundering and terrorist financing, including the duty to report, the obligation to perform more substantive background checks on customers and on third parties participating in transactions, and the obligation to identify politically exposed persons (PEPs).

Considering the position of Estonia on the periphery of the European Union (EU) and its border with Russia, sufficient risk and vulnerability exists in the movement of cash whereby finances of unknown origin might reach dealers through the services and goods they offer, therefore legalising money of illegal origin. Additionally, risk and vulnerability exists in using the freedom of movement in EU and the lack of checks on the borders between EU states to transport cash with the purpose of converting it into valuable goods, maintaining the option to sell these valuable goods for cash in another state and converting the assets of illegal origin into legal money. At the national level, it is necessary to consider in which field the dealers operate and which products/services they offer. Companies selling precious metals/stones and luxury goods will always pose greater risks. Similarities can be seen with providers of some beauty services/products where the procedures or products are expensive. The risks are lower in the retail sector. Among car dealers, the use of cash (i.e. paying in cash when purchasing a vehicle) is brought to a minimum, but additional clarification and training is fully appropriate to reinforce knowledge and improve awareness of risks and vulnerabilities from money laundering and terrorist financing in the sector.

Therefore, one possible money laundering risk scenario is based on cash transactions (above EUR 10,000).

### **Transactions involving gold, diamonds, other high-value lifestyle goods, stolen or robbed antique items and other high-priced works of art**

Transactions involving assets similar to cash (e.g., gold, diamonds), high-value lifestyle goods (e.g., cultural objects, cars, jewellery, watches), but also stolen or robbed antique items and other high-priced works of art also pose potential risk due to a low level of control. Gold is an extremely attractive method of money laundering. Gold ensures organised crime groups the means by which illegally obtained money is converted into a stable, anonymous, convertible, and easily tradeable asset for the purpose of selling for criminal proceeds or reinvesting.

Below follows a list of indicators that may indicate activities which are related to money laundering and terrorist financing within the gold sector:

- **customer behaviour:**

- the customer (including resellers of precious metal bars) significantly increases the purchase of gold bars with no apparent reason,
- foreign citizens who purchase gold bars within a short time of period over several transactions,
- precious metal bars which are transferred between associated companies with no apparent purpose,
- the field of activity conflicts with the financial profile of the customer,
- the customer uses a P.O. box as their address,
- a previously unknown customer contacts a refinery in order to convert gold into precious metal bars.

- **company behaviour:**

- an obliged entity does not report to the FIU,
- numerous sole proprietors / private limited companies which are established by seemingly unrelated persons (powers of attorney) but which are controlled by the same groups of persons,
- wrong addresses are used to establish a company,
- a significant number of companies is established by a single natural person
- commercial activities are hard to follow – for example, there is no clarity about who organised the transport of the goods and how.

- **commercial behaviour** (also associated with trade-based money laundering):

- cash payments in large sums,
- wrong classification of purity, origin, and value of gold on customs declaration forms,
- gold is sent to a “high risk” jurisdiction in the case of money laundering or sensitive/non-cooperative jurisdictions

- **differentiation of products:**

- precious metal bars have physical characteristics that do not conform to industry standards,
- the price of gold is higher than the price of gold on the local gold market.

- **payment behaviour:**

- there are several connected entities in the payment chain,
- transit movement of financial instruments and changes in making payments,
- payments to shell companies with subsequent outgoing payments,
- granting loans (with zero interest rate) to foreign companies and natural persons,
- a natural person or a company sells gold, claiming that it originates from a location with no mining permits or from a location with no gold mines,
- international transfer of a large sum which is then quickly withdrawn in cash.

It is possible to present indicators in the diamond sector that may indicate suspicious activity and which largely overlap with those of the gold sector so they are not presented separately. However, short descriptions of the models for money laundering and terrorist financing (ML/TF) crimes are provided below:

• **Using diamonds as the payment method:**

Criminals may use diamonds to buy e.g., drugs or weapons. Diamonds may also be used to convert large amounts of cash into a compact form for easy transportation. Settlement takes place outside of financial systems and financial inspection agencies receive no information of such transactions from direct sources.

• **Purchasing diamonds to preserve illegally obtained assets:**

Diamonds are bought for illegally generated profits in order to preserve the value of the asset in the long term and, if necessary, transport them across border where it is possible to convert them back into e.g., cash.

• **Money laundering through the diamond pipeline:**

In the case of these models, the specifics related to the stages of diamond supply chains are taken advantage of. It is necessary to distinguish between money laundering crimes where the assets originate from outside of the diamond sector, and money laundering crimes where attempts are made to get stolen or smuggled diamonds and jewels back into clean circulation through a stage of the supply chain and profit from it. In the first case, both investments into diamonds and fictitious

transactions with the help of third parties are used. This is one of the most common money laundering schemes in the diamond sector and it is characterised by frequent movement of funds from account to account through various dealers, with the purpose of disguising the initial origin of the assets. Additionally, trade-based money laundering through manipulative pricing, which was addressed above, is also present here. During the recirculation of diamonds, both small-scale transactions at the private individual level (pawn shops) and large-scale reprocessing/cutting of stolen diamonds are used for the purpose of later selling them without the requirement of a certificate proving the origin of the goods. At the retail level, the scheme also described in the previous model applies: illegally obtained money is used to purchase diamonds and jewels (from shops/retail companies without a duty to report arising from specific laws, or in sums that do not exceed the reporting threshold). There have been cases where smuggled diamonds are sold in sector-specific trade fairs.

- **Trade-based model and violation of customs rules**

These models primarily cover the previously addressed schemes where the imported or produced goods are underpriced and exported goods are overpriced. In this way, it is possible to create a large amount of legal added value – this arises from the specifics of pricing. Trade-based money laundering activities include falsifying certificates of origin which help disguise the actual origin of diamonds.

- **Using financial centres and free trade zones**

Using financial centres and free trade zones in ML activities is not a model per se, but it should be considered a contributor to and a part of many of the previously mentioned models (primarily trade-based ML schemes). Trading and financial centres of the diamond sector such as Switzerland, United Arab Emirates, Israel, Belgium, and Panama allow moving large sums with a relatively high degree of anonymity.

- **Smuggling diamonds**

The goals of smuggling diamonds include realising stolen assets, preserving assets, and avoiding confiscation, thereby contributing to terrorist financing. It is also fitting to mention a TF scheme where diamonds are bought for legal money with the purpose of delivering them to a terrorist group, thereby contributing to terrorist financing.

- **TF activities using the diamond business sector**

There are significantly fewer proven cases of TF activities in the sector compared to money laundering cases. On a case-by-case basis, for example, there have been instances where diamonds associated with a terrorist group have been sold by a private individual and the finances received from the sale have been used to enter into a legal business, later its profits are again forwarded to finance the terrorist group. Using legal businesses to finance terrorist groups is a fairly common practice. A great source of risk in the diamond business comes from the fact that the cross-border transportation of means and legitimising the origin of assets is at times considerably easier compared to the other sectors.

Therefore, one possible money laundering and terrorist financing risk scenario includes transactions involving assets similar to cash (mainly gold and diamonds), high-value lifestyle goods, and also stolen or robbed antique items and other high-priced works of art.

- **Transactions concluded over the Internet**

Organised crime exhausts all possibilities to be able to integrate illegal profit into a legal form, incl. concluding and making transactions over the Internet. Cash may be used as payment for transactions concluded over the Internet.

Criminals, for example, who have received money for their illicit activities may convert it into goods that can be sold later to get back their money or transport the goods to locations where it is easier to dispose of them in the legal economy. Likewise, dealers may be taken advantage of to launder money gained from illicit activities (they find this sector attractive, unlike terrorist organisations). Consequently, risks exist that are directed against the dealers themselves where they indirectly or directly may become an accomplice in receiving illegal money, participate in money laundering or terrorist financing.

An example includes positioning Eastern or Western European financial instruments into expensive merchandise, incl. brand products (watches, purses, etc.).

Therefore, one possible money laundering and terrorist financing risk scenario is based on transactions made over the Internet, incl. dealers unknowingly committing money laundering.

#### **Using services of groups specialised in money laundering**

Among new money laundering trends, OECD has highlighted the emergence of groups specialising in money laundering, and their increased activity. In recent years, several groups whose activities are mainly directed to committing money laundering have been identified and one group has been convicted. Money laundering services have been offered to various illicit groups that have committed tax crimes, operating both in Estonia and abroad. These groups used various methods to launder money.

In one case, a network of tens of foreign companies was established with bank accounts knowingly opened in countries other than those where the companies were founded. Most bank accounts were opened in Bank Pekaos in Poland. Payment services (funnel accounts) were used to withdraw cash from the scheme (court ruling no. 1-17-6845).

In another case, a criminal group transferred sums of money from companies (construction companies) involved in a tax fraud, making payments under fictitious invoices through a “buffer” and shell companies to the bank accounts of real companies operating abroad. Usually, the money is withdrawn from the shell companies in cash and returned to the original owner. In this case, however, foreign companies received payments for goods that were not related to the construction companies involved in tax fraud. The goods were delivered to third companies in Russia. The companies which accepted the goods in Russia paid to the group offering the money laundering service in cash, which was then moved as (undeclared) cash to Estonia and returned to the persons committing tax fraud (court ruling no. 1-20-2671).

Therefore, one possible money laundering risk scenario includes the increasing use of the services of groups specialised in money laundering.

#### **Transactions with companies not liable to value added tax**

After the implementation of the appendix to the value added tax return (INF) which forms a part of the monthly value added tax return submitted to the Tax and Customs Board (TCB) which obliges companies liable to value added tax to declare data related to transaction partners and invoices, large-scale tax frauds and money laundering are relatively quickly identified by the MTA and no major damage is caused. However, this has brought about an increase in using shell companies which are not liable to value added tax as these entities do not have to submit the monthly VAT declaration. At the same time, the TCB has no access to or knowledge about what is happening on the bank accounts of these companies, thereby not being able to monitor the activities of these companies in real time. Consequently, potential tax crimes and money laundering are not quickly identifiable nor preventable, and using companies which are not liable to value added tax in order to move money is an attractive method for criminals.

Therefore, one possible money laundering risk scenario includes transactions with companies not liable to value added tax and/or money transfers to/from these companies for goods or services.

#### **Fictitious transactions between dealers and trade-based money laundering**

Fictitious transactions between dealers may take place with the intention to commit tax fraud, money laundering, or both. Tax fraud and money laundering are often committed simultaneously.

International organisations see trade-based money laundering as one of the main money laundering methods. The main reason is the difficult and time-consuming detection of money laundering, caused by long transaction chains involving companies from various countries. As goods and money move in different space at different times, it is difficult to determine whether the goods exist at all, if these are the same goods and which finances are moving in return for these goods.

From the point of view of supervision performed by the TCB, it is encouraging that by implementing the INF appendix of the value added tax return which obliges companies liable to value added tax to declare

monthly data related to transaction partners and invoices, frauds are quickly identified and no major damage is caused. However, there will always be risks. Therefore, a list of indicators is presented which may indicate a suspicion of tax fraud as well as money laundering. These indicators include unusual transactions and transaction partners such as:

- ✓ the company's low awareness about its activities;
- ✓ the transactions (products and services purchased or sold) are different from the usual activity of the company;
- ✓ no relevant documents exist related to transactions and agreements;
- ✓ transactions with offshore companies;
- ✓ transactions with persons of known criminal backgrounds or with persons associated with them;
- ✓ non-identifiable customers, lenders, suppliers;
- ✓ purchase of goods where the existence of goods cannot be proven;
- ✓ transactions with business partners or customers sharing the same address;
- ✓ payments to/from third parties who are not related to the transaction, instead, the bank account of the company is simply used to forward the received funds;
- ✓ the denomination and currency of the banknotes is not usual in the field of activity of the company;
- ✓ movements of funds in banks are not declared in the value added tax return as revenue;
- ✓ movements of funds without economic justification;
- ✓ costs which are not associated with business activities, unusual use of credit cards or other methods of taking loans;
- ✓ resolutions regarding distribution of profits which are not supported by the economic performance of the company;
- ✓ a significant rise in anonymous cash revenue, a high cash revenue from luxury goods sold, a high cash revenue from goods not actually sold (a suspicious buyer);
- ✓ very generic descriptions of high value goods listed as being sold (a lack of characteristics which would enable identification);
- ✓ invoices for sold products (goods, services) made by suspicious companies;
- ✓ the transportation costs of the company are too high compared to the value or size of the goods;
- ✓ the quantity or nature of the goods is not suitable for the method of transportation
- ✓ significant differences between the contents of customs declarations and the contents of invoices;
- ✓ significant differences between descriptions reflected in the invoices and descriptions of actual goods transported;
- ✓ significant differences between declared prices and market prices;
- ✓ significant differences between the value reflected in invoices and the insured value;

Therefore, one possible money laundering risk scenario includes submitting fictitious invoices.

## 9.3. Threats

### 9.3.1. Money laundering threats

#### **Transactions involving cash**

Cash is anonymous in nature and, consequently, there is a threat of taking advantage of dealers. The threat usually comes from the fact that criminals may want to use the dealers' sector for money laundering purposes. The dealers' sector may represent a more vulnerable sector compared to the more regulated finance sector. Once it becomes difficult for criminals to move illegal instruments in the finance sector, they may seek opportunities in the dealers' sector where the methods for preventing money laundering and terrorist financing may not be as well-regulated and their implementation may be less effective. Traditionally, one of the greatest perceived threat indicators in the dealers' sector has been the share of cash used in the sector. When dealers make transactions using the services of the finance sector, the due diligence measures applied by the finance sector also mitigate the risks of money laundering among dealers. Persons operating with the goal of money laundering are interested in the dealers' sector as cash transactions are common there, offering the possibility of avoiding the use of the finance sector entirely within the context of transactions. In Estonia's legal economy, the cash turnover is low<sup>1</sup>. On average, Estonian residents made 960,000 card payments per day in Estonia, reaching the highest level in history. The number of card payments made in Estonia in 2020 is roughly the same as a year ago (-1%). In 2020, cash was withdrawn from ATMs considerably less frequently than in the previous year (-17%)<sup>2</sup>. Based on the above, the threat involving cash transactions can be considered as „low“.

#### **Increased threats**

- the provision of a product or the making or mediating of a transaction that might favour anonymity;
- payments received from unknown or unrelated third parties;
- a business relationship or a transaction that is established or initiated in a manner whereby the customer, the customer's representative, or a party to the transaction is not met physically in the same place and whereby § 31 of the MLTFPA is not applied as a safeguard measure;
- new products, payment methods, and business practices, including the use of a new delivery mechanism or new or developing technologies for both new and pre-existing products;

#### **Transactions involving valuable goods**

Possible threats are also indicated by dealing in valuable goods such as diamonds and art, as it is easy to manipulate with high-priced and liquid goods. This primarily comes from the subjectivity of their pricing which means the goods may be manipulated by heavy overpricing or underpricing. Precious metals and precious stones are physically small high value carriers that successfully replace cash. Additionally, risks are caused by the anonymity and simplicity of dealing in goods, and the global nature of the sector. No precious metals or diamonds are mined in Estonia. Estonia is not a centre for dealing in valuable goods and the trading volumes are relatively low. Still, Estonia may be used for the transit of valuable goods.

Money launderers are not interested in goods and services with small markets. Limited options to resell goods bring risks for money launderers that may discourage them from purchasing the goods. If the market participants know each other and market surveillance is applied by the market participants in the market, it makes it complicated for money launderers to structure their transactions and lessens the possibility of a successful instance of money laundering. The internationality of the sector has the opposite effect. Successful money laundering is facilitated by the possibility of moving money across borders, concluding many transactions through long transaction chains, i.e., "layering". In some cases, money laundering is facilitated by the possibility of concluding transactions electronically from another country. Actively traded (incl. cross-border trading) high-liquidity goods with large markets may be attractive to money launderers.

<sup>1</sup> <https://statistika.eestipank.ee/#/et/p/965/r/2410/2219>

<sup>2</sup> <https://www.eestipank.ee/press/mullu-neljandas-kvartalis-suuresnes-keskmise-pangaautomaadist-voetav-summa-25012021>

**Geographical risk**

Several factors must be taken into consideration when assessing risks related to countries, geographical areas, or jurisdictions. A geographical risk arises from the geographical location. Since Estonia is a bordering country in the Schengen Area and has Russia as its close neighbour, Russia can certainly be considered as one of the geographical risks along with its citizens who might be interested in using Estonian dealers to integrate or convert assets gained from their illicit activities. Additionally, dealers need to understand and assess geographical risks in the Estonian context, such as having Russia as its bordering neighbour, being open to sea as a maritime nation (transportation of goods), having a railroad infrastructure that enables transit between Russia and Europe, and using Rail Baltic in the future which will increase possibilities for the transportation of goods. In the geographical sense, Estonia is popular in intermediary activities. Goods are mediated, mostly to Russia, and the goods themselves might actually not pass through Estonia. A persisting risk is that Estonian dealers' intermediary activities are used to transport goods with no clear overview as some countries (e.g., Russia) may not apply adequate measures to prevent money laundering and terrorist financing. An additional geographical risk is caused by sanctioned countries with restrictions set in place by the EU, UN, and US, and by countries with higher levels of corruption and other crime. In the context of terrorist financing, it is necessary to attach a geographical risk to countries which condone terrorist groups or finance terrorist activities or similar groups. Offshore / tax free and low tax territories also fall under the geographical risk. Additionally, situations may arise where according to a directive or other legislation, a territory has been classified as a low geographical risk region while Estonia might have evaluated (e.g., in a National Risk Assessment) that the territory is a high geographical risk region as it uses Estonia as a transit country or if a money laundering or terrorist financing scandal is associated with the region, making its reputation as a low risk country fall under suspicion.

Trade-based money laundering cases where illicit money is received from cross-border trade transactions, displaying various indicators (increased amounts in invoices, decreased amounts in invoices, double invoices, falsifying the names of goods, etc.), can be considered cases of average risk.

Preferably, risk and threat sources and risks related to specific activities of companies should specifically and primarily be considered within the Estonian perspective. When identifying risks related to Estonia, the following sources may be used for information: recommendations made by supervisory authorities, annual reports by the FIU, published reports, information published in the media, etc.

**9.3.2. Conclusion**

Cross-border trade is used to take advantage of the free movement of goods which allows money launderers to use international schemes under its guise, and the lack of and/or slow cooperation among various law enforcement agencies creates more favourable conditions for this. Trade-based money laundering mainly comprises taking advantage of the export and import of goods and the financial instruments of cross-border trade. At the individual level and at the level of criminal groups, risks can and must be evaluated differently, the same applies to cash or the movement of transaction funds. At the individual level (in some instances also as an organised activity), the risk mostly arises from moving cash across border. Money enters the country undeclared. Cash is used to buy luxury goods or other expensive services. There is a money laundering risk in the dealers' sector, but its level can be considered as low, because the cash turnover is low.

**Table 51.** The money laundering threat level in the dealers' sector

Sector	The money laundering threat level in the sector	
Dealers' sector	2.0	<b>average/low</b>

In general, considering the materialisation of various threats in Estonia, it is found that the money laundering threat level in the dealers' sector is **average/low**.

## 9.4. Terrorist financing threats

### 9.4.1. Low awareness of dealers and the consequent inadequacy of applied due diligence measures against terrorist financing

Terrorist financing poses a threat to the economic and political interests of the country as well as to the safety of the country and its society. The need for financing may be related to both organised terrorist groups and individual terrorists. In the case of the latter, the activities are much more difficult to identify as these individuals may be financiers, planners, and executors all in one.

Terrorist financing can take place by either transporting cash directly, or by transporting other easily tradable and liquid goods such as precious metals and precious stones. It is also possible that financing takes place through some other goods or services that are needed to plan or execute a terrorist act.

An increased level of threat is presented by the regions that host terrorist groups or that are related to terrorist financing or support. The level of threat of the region may also be increased by the central authority exercising control over its territory and by a high level of corruption. Goods that are either heading to or originating from such regions pose a risk.

Terrorist financing may mean directly delivering funds to terrorists as well as sale of goods which are acquired via terrorists (e.g., robbed cultural objects, illegally mined gold and precious stones) which terrorists use to finance their own activities.

It is important that the dealer knows and has an overview of the following:

- who and where the final consumer of the product is (the “Know Your Customer” principle) and whether the purchasing of goods has a logical connection to the consumer’s (business) activities;
- what the purpose of using the goods is;
- restrictions set on the goods (e.g., embargo requirements, restrictions on dual-use goods);
- whether the financing takes place by using logical and usual methods and means;
- whether the logistical supply chain accompanying the transaction is reasonable.

Due to their small size and high value, gold and precious stones can be easily transported across borders, both legally and illegally. Restrictions on legal transport may vary from country to country. Data collected by countries may not be adequate to identify an illegal activity. Inspecting the goods may require better prior knowledge. In illegal transport, gold and precious stones are easy to hide among the goods used as a cover. Gold and precious stones have high liquidity and their value over time is relatively high. Cross-border cash transportation generally has a stricter regulation.

As a small country, Estonia is not attractive for Islamic extremists to commit terrorist acts due to its geographical location and small Muslim community. However, large Muslim communities exist in neighbouring Scandinavia and Russia, therefore a number of Islamic extremist minded persons use Estonia as a transit country.

### 9.4.2. Conclusion

Dealers do not apply adequate due diligence measures which entails a threat that customers may take advantage of their sector. However, this threat will not take shape for most dealers as their field of activity or volumes with the customers are not so large to cause the materialisation of the risk which concerns just a few dealers (e.g., persons engaging in buying-in or wholesale of precious metals, precious metal articles and precious stones, and car dealers). The threat cannot be assessed by a single measure due to the specifics of the dealers’ sector as became evident from the NRA survey. For the dealers mentioned in the example, the threat can be considered average, and for the other dealers, low or below average.

Financial instruments are mainly of legal origin which significantly complicates the identification of terrorist financing. As the general risk in Estonia is assessed as low, the risk is also low for most of the dealers, and the risk for the dealers who are FIU subjects can be considered low or below average. The overall threat is therefore low or below average.

Threats of terrorist financing in Estonia can be considered low due to the following:

- There are no known terrorist groups operating in Estonia;
- No mining or reprocessing of gold and precious stones takes place in Estonia;
- Mining and processing of gold (mines in Finland, Russia) and precious stones (mines in Russia) in the neighbouring countries is under the control of the central government. However, precious stones from Russian mines may present some threat of illegal transportation;
- There are no large deposits of gold and precious stones in Estonia, and no large-scale dealings in such goods has taken place historically or culturally;
- There is a low level of corruption in Estonia;
- The country has control over its import, export, and transit;
- Information about sanctions (directed against what countries, goods, and persons) has been made public;
- Declaration of cash (exceeding EUR 10,000) in the context of import/export conforms to the common principles of EU, and in the near future, the data composition collected when declaring cash will be even more thorough;
- The risk assessment provided by law enforcement agencies considers the threat of terrorist financing low.

**Table 52.** The terrorist financing threat level in the dealers’ sector.

Sector	The terrorist financing threat level in the sector	
Dealers’ sector	1.40	<b>low</b>

The terrorist financing threat level in the entire dealers sector is **low**.

As a small country, Estonia is not a priority for Islamic extremists to commit terrorist acts due to its geographical location and small Muslim community. However, large Muslim communities exist in neighbouring Scandinavia and Russia, therefore a number of Islamic extremist-minded persons use Estonia as a transit country. Estonia’s innovative and well-developed dealers’ sector may be attractive to Islamic extremists in the context of terrorist financing and support. However, state’s small size and proper administration can be considered hindering to terrorist financing and support, and the threat level can be considered **low**.

## 9.5. Vulnerabilities

### 9.5.1. Vulnerabilities of prevention of money laundering

#### 9.5.1.1. Exposure to threat

##### **Transactions involving cash**

From the dealers’ perspective, the main threat is not just in using cash. A dealer becomes subject to the MLTFPA when making a cash transaction above EUR 10,000. Cash is conspicuous and upon owning it, the purpose is to convert it into another value. Money (in this case, cash) gained through illicit means is sought to be put into products and services. The threat arises from dealers not adequately assessing customers’ behaviour and their intentions, and large sums of money may be placed in provided services or products (the dealer’s obligation to apply due diligence measures).

Another threat arises from the unawareness of dealers and their exploitation. A picture is painted for dealers in such a way where they might not realise that they and their services are being used to launder money. It became clear from the survey that 1.32-5.13% of the respondents operated with cash (above EUR 10,000) within the last year (2019-2020) which shows that the share of cash in the dealers' sector has already been brought down to a minimum. As the euro is used as cash in 19 member states and its cross-border movement is not traceable, it is not possible to evaluate the current amount of cash in circulation in a given member state. In the Eurozone, 1.29 trillion euros worth of banknotes are in circulation and the amount has increased by 5% per year. Since joining the Eurozone, the Bank of Estonia (Eesti Pank) has emitted banknotes worth over 2 billion euros. By considering various statistics, it can be assumed that the volume of cash in circulation has increased just slightly. For example, the yearly increase in cash withdrawn from ATMs has been between 1% and 2.5%. Cash transactions were made by 58.5% of the survey respondents. Of all the respondents, 3% stated that they had concluded a cash transaction with their customers and/or suppliers in an amount above EUR 10,000 during the year preceding the survey (either as one payment or as the sum of several linked payments).

According to a European Commission report, the risks for and vulnerabilities of dealers dealing in luxury goods / high value goods / precious stones and metals, gold and diamonds, are as follows<sup>3</sup>:

- Criminals who have gained cash proceeds from their illicit activities, intend to convert it into goods that can be sold when necessary to regain the money, or to move them to locations where one has easier access to placement in the legal economy
- It is the goal of organised crime to take advantage of dealers in order to launder money gained through illicit means (they find this sector attractive, unlike terrorist organisations)
- Converting cash into valuable goods, transporting goods across border, and converting goods back into cash is easy due to a lack of effective control measures;
- Risk for terrorist financing is low as the use of cash is preferred here;
- Using cash poses risks and increases vulnerability;
- Risk awareness is low;
- There are no checks in place at the EU's external borders (e.g., declarations)

Measures:

- ✓ A common cash control regulation;
- ✓ Increasing awareness in the sector;
- ✓ Facilitating cooperation between the public and private sector;
- ✓ Encouraging cooperation between law enforcement agencies at the national and cross-border level.

### 9.5.1.2. Risk awareness

#### **Management commitment and leadership**

Dealers who conclude cash transactions above EUR 10,000 (in one payment or in total) must organise risk assessment procedures and consider their customers and other accompanying risks. To do this in an efficient manner, it is necessary for the management to be aware, train their employees, be a member of umbrella organisations, and have the will to comply with applicable rules and law. A majority of the questionnaire respondents did not have a monitoring system in place and were not keeping up with the topic of money laundering.

Most dealers do not have and indeed do not need activity licences. As only some dealers have activity licences (e.g., alcohol sales) and the requirement for an activity licence depends on the subsector, it is not possible to get an overview of the dealers' sector based solely on licences. Activity licences generally do not address questions related to money laundering and are established by the state for other purposes. An exception is the activity licence issued by the FIU for the buying-in or wholesale of precious metals, precious

<sup>3</sup> European Commission's report 2019, pp 150-170

metal articles and precious stones, which is a relevant activity licence in the context of preventing money laundering.

Less than half of the respondents who are obliged entities perform employee background checks and a third of obliged entities evaluate the trustworthiness of employees during the employment relationship. Of the survey respondents who are obliged entities, 8.2% stated that their employees who are responsible for the prevention of money laundering undergo training. 21.6% of the responding obliged entities dealt with other know-how related to employees and their prevention of money laundering. Obligated entities mostly responded that the members of the management board of the company were responsible for the prevention of money laundering. Of the survey respondents who are obliged entities, 22.7% stated that their company had applied rules of procedure for the prevention of money laundering and terrorist financing, and guidelines for reporting suspicions of money laundering or unusual transactions. In practice, 4.5% of the responding obliged entities have needed to use these guidelines. 7.2% of the responding obliged entities have felt the expectations, assumptions, and requirements to comply with standards against money laundering that were expressed by transaction partners and other market participants, mainly from the finance sector. However, the actual impact on the activities has been insignificant.

Risk awareness is also characterised by the activities of representative organisations. The dealers' sector is diverse and there is no single representative organisation that covers all dealers. There are numerous representative organisations and their level of professional and ethics standards as well as their activity and inclusion of the subsector vary. Some subsectors do not have a representative organisation. Of the survey respondents who are obliged entities, 10.3% stated that the representative organisations of the sector have established guidelines for preventing money laundering, of which 90% found that these guidelines have been useful. 7.3% of respondents of the survey, who are obliged entities, knew that in their field of activity take place thematic roundtables, discussions, and other forms of cooperation to prevent money laundering. Thus far, the role of professional organisations in the dealers' sector related to the prevention of money laundering has either been rather small or the dealers have not been aware of the activities of these professional organisations. A good example of a representative organisation working in the sector which contributes to the prevention of money laundering is the Estonian Vehicle Dealers and Services Association which is active in both training the sector and standing up for its interests. An association's self-regulation principles are included in its articles of association. The Estonian Chamber of Commerce and Industry has also contributed to the topic of prevention of money laundering both substantively (through opinions on draft acts) and by offering training for dealers (incl. in collaboration with the FIU and the Ministry of Finance). The Estonian Chamber of Commerce and Industry is the largest umbrella organisation for dealers, its members including more than 3500 active companies (~40% of companies).

#### **Brief summary**

Low awareness in the dealers' sector regarding the risks of money laundering can be considered its greatest vulnerability. The sector is large and many of its dealers are smaller companies whose capability of preventing money laundering is insufficient due to their low resources. As dealers are usually not obliged entities, specific knowledge related to preventing money laundering is not necessary. However, the survey indicated that this awareness was not very high among obliged entities, either. Dealers' awareness about when to report a cash transaction is of key importance in the prevention of money laundering within the dealers' sector. This aspect requires a solution at the national level.

### **9.5.1.3. Legal framework and control**

#### **Quality of supervision**

Regarding the prevention of money laundering, the sector is mainly regulated by the MLTFPA. Companies operating in the field of precious metals have additional obligations arising from the Precious Metal Articles Act. No sector-specific regulation exists in Estonia for the dealers of precious stones.

Supervision over the dealers is exercised by the FIU. The general competence of the FIU arises from § 54 of the MLTFPA. There are no organisations applying additional regulations or standards.

The risk-based approach provided by the MLTFPA is applied to the dealers when a large-scale cash transaction takes place and when the dealers are obliged to apply due diligence measures in accordance with the MLTFPA. § 56 of the MLTFPA provides that the FIU has the right to issue advisory guidelines to explain legislation preventing money laundering and terrorist financing. These guidelines and the FIU training take a risk-based approach. The following guidelines and recommendations are relevant to the dealers in preventing money laundering:

- Guidelines for submitting a report to the FIU;
- Guidelines on the characteristics of suspicious transactions;
- FIU recommendations for the management of risks arising from the activities of obliged entities;
- FIU recommendations for the preparation of the rules of procedure and internal control rules.

The survey indicated that most dealers who are obliged entities were not aware of the FIU guidelines and recommendations. Of the survey respondents who are obliged entities, 13.4% knew that the supervisory authority had prepared relevant guidelines and recommendations for their sector. These guidelines and recommendations were considered useful by 38.5% of those who were aware of the existence of the guidelines and recommendations.

The FIU exercises risk-based supervision over the dealers' sector. Cross-border cooperation takes place in an official capacity as well as informally. As the dealers' sector is large, with many market participants and subsectors that differ from each other significantly, it is difficult to provide a general picture of the sector. Additionally, supervisory authorities find it difficult to identify which dealers are obliged entities. Consequently, supervisory authorities do not have a good understanding about the obliged entities within the sector. Active supervision has mainly been targeted towards subsectors with more large-scale transactions – dealers of valuable goods and vehicles.

One of the most difficult challenges is how to identify obliged entities in the dealers' sector as no automatic mechanism exists which could identify a large-scale cash payment taking place. At the moment, it is necessary to use the reports submitted to the FIU by the market participants themselves, in order to outline the obliged entities. During the observed three years, dealers submitted 152 sum-based reports. 3393 persons (approx. 9% of the total sample) responded to the survey prepared for the risk assessment, and just out of these respondents, 97 persons should have submitted sum-based reports. The survey sought answers for the previous year, a period three times shorter than the one observed in the report. Additionally, dealers must submit a sum-based report for each large-sum transaction made in cash so one dealer may have submitted several reports. If the low awareness of money laundering risks within the dealers' sector is added to this equation, it can be concluded that the supervisory authority identifies only a fraction of all cash transactions above EUR 10,000 in the dealers sector. There is also no overview about whether there are sectors where the respective cash payments take place, but so far no cash payment reports have been made.

The response of the FIU to the cash reports also depends on the number and volume of these reports. The FIU is not obliged to respond to a cash report and indeed does not respond to every individual cash report. The reaction of the FIU is based on the extent of the activity of the obliged entity, its behaviour pattern, and other case-related circumstances. The effectiveness of risk-based supervision depends on the quality of the information available.

In 2017-2019, the FIU received eight reports of suspicion of money laundering, two reports of unusual activities and two reports of unusual transactions. Precious metal dealers have submitted three reports of suspected money laundering and two reports of unusual activity. All reports from precious metal dealers were submitted in 2019. The FIU has carried out one on-site inspection at dealers in precious metals, seven on-site inspections at other dealers, during which seven violations were identified. No remote inspections have been performed. The FIU conducted a total of five misdemeanour proceedings against dealers, fines were imposed in the total amount of EUR 760.

The FIU also keeps track of open case studies in the sector. In the statistics collected, the sectors of the reports have been categorised. There were eight files related to reports of dealers of cars and other vehicles

in 2017, seven in 2018, and five in 2019. Regarding other dealers, one file has been open during each year observed. Due to the risk-based approach and the limited resources of the FIU, the activities of the FIU in the dealers' sector have so far been mainly reactive. Reports are responded to and processed in accordance with the law, but resources have not been sufficient to initiate activities on their own initiative alongside other sectors. Car dealers are an exception here, being the main targets of supervisory activities. Consequently, the majority of companies in this sub-sector have abandoned cash transactions. The survey indicated that just a few obliged entities in the dealers' sector have used the reporting system, as one tenth of the respondents were able to rate its user-friendliness, but those who had rated it were satisfied with the technical functioning of the system and found it convenient.

In order to facilitate supervision and determine liability, and in accordance with § 17 (1) of the MLTFPA, where the obliged entity has more than one management board member, the obliged entity appoints a management board member who is in charge of the implementation of the MLTFPA, and legislation and guidelines adopted on the basis thereof. The MLTFPA prescribes penalties for failure to fulfil obligations for both legal and natural persons. The Penal Code provides additional punishments for money laundering and for the conclusion of an agreement on money laundering. Considering that Estonian dealers are mainly medium and small-sized companies, the extent of the punishments is adequate. Members of the management board have been mentioned as the necessary elements of criminal offences, but top management is not mentioned in this context. In practice, there have been cases where the supervisory authority identifies the violation of an obligation set forth in the MLTFPA, but the violation does not comprise any necessary elements of an offence. The FIU has also imposed penalty payments, but the options for collecting penalty payments are limited due to which the penalty payments have not been paid. This is relevant mainly in the cases where the management of the legal entity is located abroad.

From a national perspective, the vulnerability of the dealers' sector, compared to other sectors, is below average.

The FIU has performed supervision over its subjects sufficiently, but recently (since the start of issuing the activity licences) the resources of the FIU have been limited due to its activities being directed elsewhere and therefore its supervision has become less intensive, but the subjects under the supervision of the FIU (from the dealers' perspective) are adequately trained and inspected to ensure above-average satisfactory behaviour and activities by dealers. Car dealers and higher-volume dealers, for example, have sufficient knowledge. Dealers who make one-off or rare cash transactions with their customers above EUR 10,000 have less sufficient knowledge and background.

### **Effectiveness of compliance control systems and reporting**

When preventing money laundering, it is important that the information indicating possible money laundering discovered in the course of the company's activities reaches the supervisory authorities. For this purpose, a duty to report has been established in the MLTFPA to obliged entities. In order to implement the duty to report in the best possible way, public authorities need to create an environment in which dealers and dealers' employees should not fear regulatory sanctions if they act responsibly and apply adequate due diligence measures. It is important for the functioning of the system that regulatory sanctions are not applied, but dealers must also be aware of this. Additionally, dealers need to be aware that reports are processed by ensuring confidentiality of the person submitting the report. Of the survey respondents who are obliged entities, 7.2% thought that reporting a suspicion of money laundering could bring negative consequences for the employee submitting the report and 19.6% thought that reporting could bring negative consequences for the company. Given that 29.9% and 33% of the respondents, respectively, could not answer the above questions, it can be stated that in almost half of the cases in the dealers' sector, the person who received information about money laundering was not aware of the protection offered to a person reporting money laundering.

The FIU is not obliged to respond to the submitted reports so dealers have not received individual feedback on the reports. In 2020, the FIU provided sector-based feedback to the dealers' sector, see <https://www.fiu.ee/aastaraamatud-ja-uuringud/>. In some cases, feedback may improve the prevention of money laundering and increase the likelihood of receiving reports from the same dealer in the future.

Awareness can be raised by training that is provided by both public and private sectors. During the observed period, the FIU conducted two training courses for dealers with around 80 participants. The training attracted the audience. 8.2% of the survey respondents, who are obliged entities, responded that their employees responsible for the prevention of money laundering undergo training. 2% of all respondents of obliged persons answered that their employees are trained in preventing terrorist financing and money laundering at the FIU and/or Internal Security Service (ISS). Therefore the trainings have been aimed mainly at dealers of high-value goods.

The precondition for sending notifications to FIU is that the dealer is able to identify situations where the risk of money laundering is higher. As well as the other sectors, dealers rely partly on due diligence measures applied in the financial sector. This is not possible with cash payments. The survey indicated that the verification of the origin of the funds, the purpose of the transaction, and the final beneficiaries of the transaction partners is carried out by obliged entities to the extent deemed necessary by the obliged entity to ensure that the transaction partner fulfils its contractual obligations. Dealers have limited opportunities to identify and analyse complex and unusual transactions. Additionally, dealers who are obliged entities are not aware of the obligation to identify politically exposed persons and the additional due diligence measures associated with them. It can be concluded from the responses to the survey that few dealers identify PEPs, as 83.5% of the respondents could not evaluate the availability of the information needed to identify PEPs.

Changes have been introduced to the MLTFPA, as a result of which the FIU provides feedback to the subjects on an ongoing basis (regarding the reports submitted by the subject as well as generally) and via the FIU yearbook. Additionally, there are specific plans to involve umbrella organisations in training. From 2021, the FIU wants to invest more in organising training and will seek to raise awareness in the sectors. The vulnerability is evaluated to be below average.

#### **Quality of the framework of due diligence measures applied to the customers**

The primary level in ensuring the quality of money laundering prevention comprises the dealer itself operating in the sector. The secondary level in ensuring the quality of money laundering prevention is cooperation with supervisory and investigative authorities. However, the most effective way to prevent money laundering is to sell services or goods above EUR 10,000 only using bank transfers. Little or no use of cash by dealers makes it difficult, if not impossible, for the criminal world to make use of cash. The use of cash is low in the sector with more expensive products, and the customer-related risk mitigation (using the risk-based approach) is done via internet searches and, in some cases, with the help of KYC questionnaires.

Performing customer due diligence is partly limited by the characteristics of the dealers' sector. This is a sector characterised by a high level of competition and brief contacts with customers. Some customer relationships are long-term, but these cases mostly comprise individual transactions where it does not take long between the first contact and the conclusion of the contract. Of the survey respondents who are obliged entities, 7.2% make their own efforts to identify the origin, purpose, and beneficial owners of the funds in higher risk cases. 12.4% consider the information on the beneficial owners of legal persons in the national register to be reliable, while 84.5% could not provide an answer. 22.9% of the respondents consider the information on the beneficial owners easily accessible. 25.8% of the respondents consider the Estonian information systems used for checking customer data to be thorough and reliable and 63.9% could not respond to the question. Information regarding the identification and checks of high-risk customers was considered accessible only to 9.3% of the respondents.

The results of the survey indicate that only a few obligated dealers perform customer checks and take the necessary steps therein to prevent and monitor money laundering. As a rule, dealers do not have to apply due diligence measures prescribed by the MLTFPA, but the respondents who answered to this question in the survey had also been obliged entities within the meaning of the MLTFPA during a transaction at least once during the last year. As many dealers are rarely obliged entities, they cannot develop a so-called "skill" in mitigating money laundering risks. The inability to identify PEPs and beneficial owners means that dealers cannot assess the level of risk of the transaction. Performing customer checks becomes even more

difficult when offering cross-border goods and services, especially for small companies which can offer their goods and services in various countries with the help of e-commerce solutions. Additionally, it is worth noting that none of the respondents to the survey considered the risk-based approach to combating money laundering to be simultaneously clear and applicable.

Dealers become obliged entities within the meaning of the MLTFPA only when the transaction is above EUR 10,000. In order to ensure the application of due diligence measures, it is necessary that dealers know and become familiar with the law, be up to date with various risks and, to minimise the risk involving cash, avoid making large-sum cash transactions if possible.

The vulnerability is evaluated to be average or below average. Many of the dealers are not subjects. The FIU has reached the subjects at some point over the course of supervision and shared additional information to help identify and explain larger risks.

#### **9.5.1.4. Sector-specific risk assessment with the quality of sector-specific controls**

From the dealers' perspective, the main threat is not just in using cash. A dealer becomes an MLTFPA subject when making a cash transaction above EUR 10,000. Cash is conspicuous and upon owning it, the purpose is to convert it into another value. Money (in this case, cash) gained through illicit means is sought to be put into products and services. A threat arises from dealers not adequately assessing customers' behaviour and their intentions, and large sums of money may be placed in provided services or products (the dealer's obligation to apply due diligence measures).

Another threat arises from the unawareness of dealers and their exploitation. A picture is painted for dealers in such a way where they might not realise that they and their services are being used to launder money. By using the sector-specific risk identification quality ECRAT, the efficiency rating is between 2 and 4 which means that controls have been designed in an at least satisfactory manner and their efficiency is 50-75%.

It became clear from the surveys that 1.32-5.13% of the respondents had operated with cash within the last year (2019-2020) which shows that the share of cash in the dealers' sector has already been brought to a minimum. It can be concluded that vulnerability is low, as the share of cash is very small and therefore the level of threat is low.

#### **9.5.1.5. Quality of the response to risks identified in previous evaluations**

The results of NRA 2015 indicated that the level of vulnerability of the sector had the Domestic Cooperation rating of 0.75 (average/high) during the last assessment period. Deficiencies were mainly related to technical aspects (e.g., access to some information is limited at the moment) which is solvable in practice but these developments require additional resources. The following proposals were made:

- To analyse options for creating access to the MIS platform for the Tax and Customs Board which contains information about initiated money laundering investigations.
- To analyse options for regulating systematic operational information between the Tax and Customs Board and the FIU.

The relative size of shadow economy was assessed (input was given by the Tax and Customs Board and Ministry of Finance). According to the Tax and Customs Board's evaluation, the tax gap in 2011 was 422 million EUR or 26% of the GDP. The year before, it was 481 million EUR. The reduction in the size of the tax gap in 2011 arises from the reduction of losses in income tax, social tax, and fuel excise duty. The losses of value-added tax increased by 8 million euros but considering the overall development of the economy this amount is not significant. The main change in the tax gap structure was the proportional increase in value-added tax losses, reaching over 50% of the entire tax gap (value-added tax losses comprised 54% of the tax gap) which was caused primarily by the decrease in the losses of the other taxes rather than the increase in the losses of value-added tax.

According to the Estonian Institute of Economic Research, shadow economy made up 8% of the GDP in 2012. By assessing the proportion of shadow economy in residents' purchases, it can be concluded that by comparing the years 2010 and 2011, the share of those consumers who base their decisions only on the cheaper price of the goods and services and do not consider their potential illegal origin, has decreased. The ratio of the respondents who made their decisions only based on the price, decreased to 13% in 2011 (18% in 2010).

In 2011, 17% of illegal envelope wage earners received on all of their income via envelope wages, which is more than in 2010 (11%). According to the NRA 2015 methodology, the Estonian indicators scored 0.9 (high). A proposition was made in the NRA to continue preventing shadow economy. In the IMD "World Competitiveness Yearbook 2017", Estonia is among the average in terms of the detrimental effect of shadow economy – Estonia ranked 34<sup>th</sup> among 61 countries (32<sup>nd</sup> place in 2016), Switzerland ranked 1<sup>st</sup>, Finland ranked 2<sup>nd</sup>, Latvia ranked 47<sup>th</sup>, Lithuania ranked 50<sup>th</sup>. In terms of tax evasion, Estonia ranked 25<sup>th</sup> in 2017 (27<sup>th</sup> place in 2016, 28<sup>th</sup> place in 2015), Latvia ranked 55<sup>th</sup>, and Lithuania ranked 50<sup>th</sup>.

Regarding the NRA 2015, the vulnerability of the dealers' sector (precious stones and gold) was rated M (medium). Recommendations to influence or change the situation: training, supervision, and updates/amendments to legal acts. As for the dealers (cars and boats), considering the structural indicators as well as control measures, the vulnerability of the sector was rated ML (medium low). Recommendations to influence or change the situation: training and supervision. As for the dealers (art and antiques), considering the structural indicators as well as control measures, the vulnerability assessment of the sector in this module was ML (medium low). Recommendations to influence or change the situation: training. Overall score for the structural indicators of dealers (scrap metal) was M (medium). Recommendations to influence or change the situation: training, supervision and updates/amendments to legal acts.

To get a better overview, risks must be assessed regularly – therefore, the risk assessment should be updated on a regular basis.

### 9.5.2. Conclusion

It is the first goal of a money launderer to conceal the proceeds of crime by channelling it into the legal financial system and economy. Therefore, it is important in the money laundering context that transactions look similar to legal economic transactions. Money laundering transactions should not be obvious to those parties whose duty it is to identify them. However, certain differences do exist as it is not reasonable to perform money laundering transactions with the same level of detail. Law enforcement agencies need to understand whether transactions seem viable and plausible and make economic sense. It is therefore necessary to view the contents of the transaction and compare it to other real transactions in the same economic sector, to make sure that other market participants would act the same way, and to determine the business rules, agreements, standards, and documentation prevailing within this specific field of activity.

From the dealers' perspective, one significant aspect is the external vulnerability. Organised crime exhausts all possibilities to be able to integrate illegal profit into a legal form. In this case, it is important to offer training to dealers and raise their awareness so that the companies operating in the sector nationwide could clearly and unambiguously understand the risks that are directed against the dealers themselves where they indirectly or directly may become an accomplice in receiving illegal money, participate in money laundering, or terrorist financing. It could be said that not all money is welcomed, even though the temptation may arise, depending on the offers.

On a scale of 1 to 5, the level of vulnerability in the dealers' sector from the money laundering aspect is 2.59, i.e., **low**.

**Table 53.** The money laundering vulnerability level in the dealers' sector.

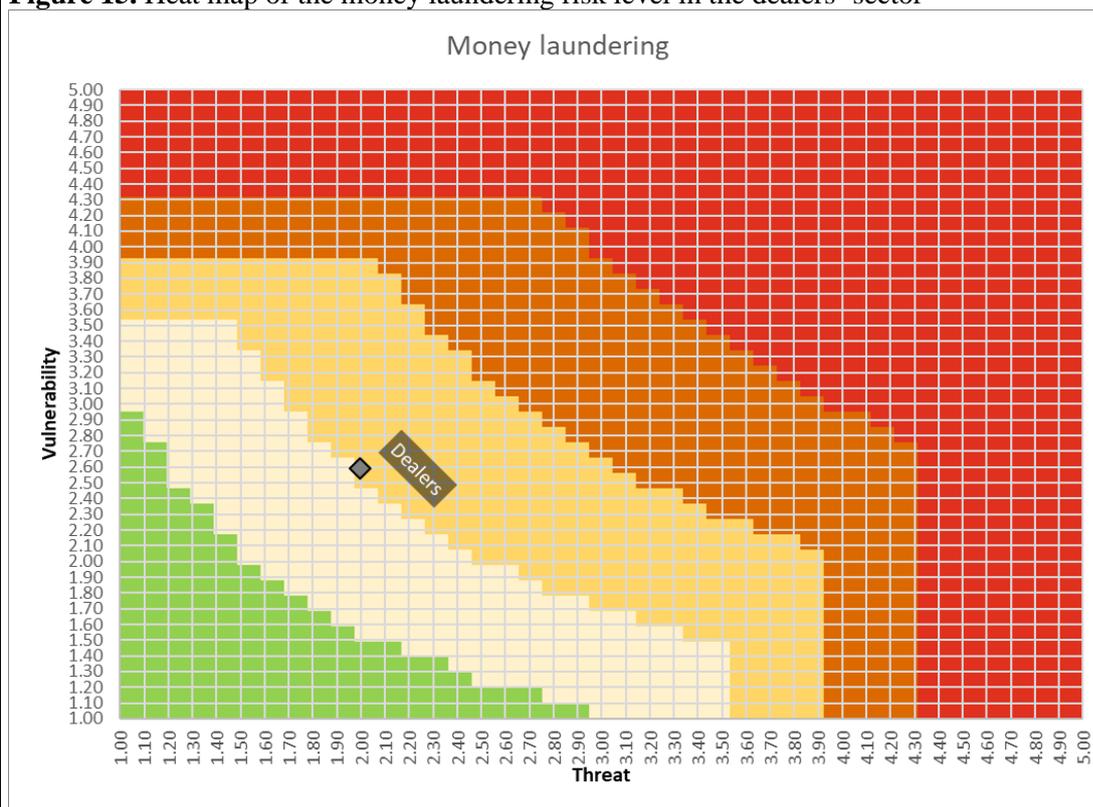
Sector	The money laundering vulnerability level in the sector	
Dealers	2.59	<b>low</b>

The precious metal and car dealers' subsectors can be considered the sector's strengths as they have performed supervision on a more regular basis, and laws have been amended to ensure the efficiency of combating against money laundering (precious metal dealers).

Art dealers, for example, could be considered more vulnerable – they are considered obliged entities if they make transactions above EUR 10,000. It is important to train dealers and introduce to them the topic (e.g., management commitment, etc.). Additionally, it is important to train the entire sector to explain to the companies in the sector when they become subjects and what the key activities in preventing money laundering are. It can be concluded from the responses to the questionnaire that the awareness of market participants within this sector should be raised. One of the weaknesses considered is access to information about beneficial owners and PEPs both nationally and internationally. This aspect needs solving at the national level.

Even though the level of vulnerability in the sector is low, the emphasis must be given to training to raise awareness as it would help maintain the current low vulnerability level.

**Figure 15.** Heat map of the money laundering risk level in the dealers' sector



**Summary**

The risk level in the sector from the aspect of money laundering is **below average** which means that it is necessary to address the mitigation of the existing risk and to apply specific measures. Simplified due diligence measures may be applied in the sector.

### 9.5.3. Risk management strategy

#### 9.5.3.1. Risk mitigating measures at the state level

Based on the results of the risk assessment, the following proposals are made to improve the situation on the state level:

- Provision of automated responses by the FIU to the persons submitting reports (confirming that the report has been received and providing feedback, if possible);
- Business register: organising information about beneficial owners (so that 100% of the beneficial owners are represented), verification (data corresponds to reality), imposing more severe relevant punishments (amending legislation), updating. Associating involvement with beneficial owners;
- In the longer term, data needed for the application of due diligence measures should be accessible from a single web portal;
- Data from the national registers that is needed for the application of due diligence measures should be provided to the obliged entities free of charge or on more favourable terms;
- Provision of sector-specific guidelines to the market participants (provided by the FIU).

#### 9.5.3.2. Risk mitigating measures at the level of obliged entities

Based on the results of the risk assessment, the following proposals are made to improve the situation at the obliged entities level:

- Raising sectoral awareness through training and roundtables provided by the supervisory authorities (FIU);
- Providing training for the employees of companies through the FIU and umbrella organisations (Estonian Chamber of Commerce and Industry, Estonian Vehicle Dealers and Services Association, etc.).

### 9.5.4. Vulnerabilities of prevention of terrorist financing

#### 9.5.4.1. Exposure to threat

Low awareness of dealers and the consequent inadequacy of the applied due diligence measures against terrorist financing: the results of the survey conducted by the NRA among market participants show that due to the typologies of terrorist financing, market participants demonstrate difficulties in identifying suspicions of terrorist financing and in finding potential and relevant connections. In 2017-2019, dealers submitted two reports to the FIU about a suspicion of terrorist financing.

Terrorist financing can be difficult to identify as the value of identifiable transactions can be relatively low. Funds can come from both illegal and legal sources. In the case of the latter, it is much more difficult to find a link between terrorist financing, and such transactions do not have the characteristics of money laundering transactions. Goods and services acquired for terrorist financing may not be criminal in nature or directly related to the organisation of a terrorist act, but may be related to the financing of the day-to-day activities of terrorist organisations, such as buying food, vehicles, fuel, clothing, etc., and financing travelling and training. The final purpose for which the goods or services will be used may become decisive.

During the last year, the majority of the companies responded (approx. 95%) have not made a cash transaction or several connected cash transactions above EUR 10,000. Transactions have been above EUR 10,000 in 3% of the cases, EUR 32,000 in 1% of the cases, and EUR 100,000 in less than 1% of the cases.

Scandals in Estonia have affected both the public and, obviously, the dealers. The due diligence measures applied and a more conservative approach to non-residents and e-residents also significantly reduce the level of threat related to terrorist financing among dealers (car dealers have more control over the origin of assets and performing checks on foreigners for any background potentially involving a terrorist threat). At the same time, the competitive environment pressures acting in an innovative way by working with customers across borders. A large amount of cash carries a high risk (unknown origin), the customer's background is not always unambiguously identifiable (non-residents). However, the vulnerability of preventing terrorist

financing is average due to the relatively low risk. This in turn arises from the fact that the Estonian dealers' sector is not attractive enough for Islamic extremists in the context of terrorist financing and support, therefore, the level of threat should be assessed as low or below average.

#### 9.5.4.2. Risk awareness

##### **Management commitment and leadership**

The results of the survey prepared for the NRA indicate that awareness of the management regarding the prevention of terrorism and their management role varies among different subsectors. On average, 43% of the respondents assured that the management has a decisive role in the prevention of money laundering and terrorist financing as well as complying with sanctions (64% and 52% of companies dealing in precious metals and vehicles, respectively). However, 46% of companies have not appointed a person in charge of the prevention of money laundering and terrorist financing and complying with sanctions. Reasons include the lack of practical cases and the need to do so.

In 2019, no reports related to the suspicion of terrorist financing were submitted to the FIU by the dealers' sector (in 2019, a total of 4 reports related to the suspicion of terrorist financing were submitted to the FIU).

The greatest vulnerability comprises the inadequate awareness of dealers and the accompanying inadequacy of applying due diligence measures against terrorism. The sector is large and many of its dealers are smaller companies whose capability of preventing money laundering is less sufficient due to their low resources. However, such specific knowledge is not even necessary for many of the dealers.

#### 9.5.4.3. Quality of terrorist financing detection and prevention financing of proliferation of weapons of mass destruction

##### **Quality of supervision**

The controls comprise assessments of mainly two aspects: the level of regulations and the adequacy/inadequacy of supervision.

The regulations related to the prevention of terrorist financing are adequately efficient.

From the supervisory perspective, the key problem is the inadequacy of human and technological resources, or less sufficient skills and knowledge for using the existing resources. As the sector is broad, the quality of performing supervision varies significantly within the sector. There are few subsectors with sufficient knowledge and skills.

Legal regulation is sufficient. Less sufficient knowledge and skills of the market participants in applying the measures prescribed by the regulations is problematic.

##### **Effectiveness of compliance control systems and reporting**

Detecting terrorist and proliferation financing is certainly a hard task for dealers as financing may take place by "non-sanctioned" persons, either knowingly or not. See also section 9.4.1.

- *Investments by top management to risk management technologies (feedback from the market participants)* No investments are made to the technical solutions of risk management by the market participants. However, this may not automatically indicate a high risk as information about sanctioned persons and restrictions is available from various public sources (e.g., sanctions lists).
- *Identifying politically exposed persons (how the systems work from the perspective of the sector's market participants)* Awareness varies within the dealers' sector. However, most sectors are generally not familiar with the requirement of identifying politically exposed persons. A helpful solution would be to develop a (simple) IT system which facilitates identifying such persons.

- *Availability of mechanisms identifying complex or unusual transactions in the sector (feedback from the market participants)* In the case of complex or unusual transactions, market participants may not be able to identify the risks associated with terrorist financing or proliferation financing.

Identifying terrorist financing and proliferation financing is a difficult task for dealers. A helpful solution would be to develop a unitary and easy-to-use IT system.

#### **Quality of the framework of due diligence measures applied to the customers**

Dealers are generally aware of the duty to report to supervisory authorities if the suspicion of terrorist financing arises during a transaction with the customer or if the unusual transaction is related to areas of higher terrorist threat or high-risk countries. However, in reality, this has not been done whether due to a lack of the problem or due to inefficiency of identification. The information systems used for identifying high-risk customers and checking the customer data could not be evaluated due to a lack of experience and knowledge.

Vulnerabilities include difficulties in accessing information in the event of suspicion of terrorist financing.

- Information contained in the national registers about beneficial owners is not always trustworthy;
- It is difficult to access information needed for identifying the beneficial owners;
- It is difficult to access information needed for identifying and checking other high-risk customers (e.g., embassies, virtual currency service providers, companies providing financial services, non-profit associations, etc.).

In a real situation, dealers may not be able to identify all the risks associated with a customer and may be vulnerable when applying customer due diligence. As for customer background checks, the problem arises from the lack of a register of PEPs, as well as the complexity of the process of identifying beneficial owners and the lack of a reliable source.

Taking into account the general low level of terrorist financing in Estonia, it can also be considered low in the dealers' sector.

#### **9.5.4.4. Quality of the identification of sector-based international sanctions**

The results of the survey show that the awareness of the existence of the sanctions list is generally low and the comparison of lists/products/persons in companies is not firmly established by the internal work organisation. Although it can be assumed that the dealers' sector generally has no exposure to dual-use items, various sanctions may comprise individuals as well as other "regular" goods which, depending on the origin or destination country, may be sanctioned.

Awareness of sanctions in the dealers' sector is low, verification of the existing sanctions and reporting sanctions-related cases do not function in an efficient manner.

#### **9.5.4.5. Sector-specific risk assessment with the quality of sector-specific controls**

The following vulnerabilities have been identified in the analysis and the assessment of sector-specific risks:

- Lack of (or insufficient) awareness about international sanctions lists designed to prevent terrorist financing or violations of international sanctions in transactions.
- Lack of (or insufficient) awareness about the availability of sources enabling identification of existing sanctions.
- Insufficient awareness about dual-use items.
- As can be concluded from the questionnaires, in most cases the relevant methods for determining the origin and purpose of financial instruments and beneficial owners in high-risk cases are not used.
- Insufficient awareness of the mechanisms and user-friendliness of submitting reports to the FIU.
- Insufficient awareness about PEPs.

Considering the context of dealers, it is clear that there is a lack of or insufficient knowledge about sanctions lists, and options for searching for politically exposed persons, which may be due to dealers not having to

or not having the opportunity to be exposed to these circumstances, or they may be unable to identify these circumstances in transactions.

#### 9.5.4.6. Quality of response to risks identified in previous evaluations

The previous evaluations of terrorist financing in the dealers' sector were not sufficient.

#### 9.5.5. Conclusion

On a scale of 1 to 5, the level of vulnerability in the dealers' sector from the terrorist financing aspect is 2.59, i.e., **low**.

**Table 54.** The terrorist financing vulnerability level in the dealers' sector.

Sector	The terrorist financing vulnerability level in the sector	
Dealers	2.59	<b>low</b>

The small proportion of cash and the low volume of transactions above EUR 10,000 can be considered the sector's strengths. The legal framework is sufficient and conforming to international agreements. The transactions are based on general internationally agreed-upon thresholds.

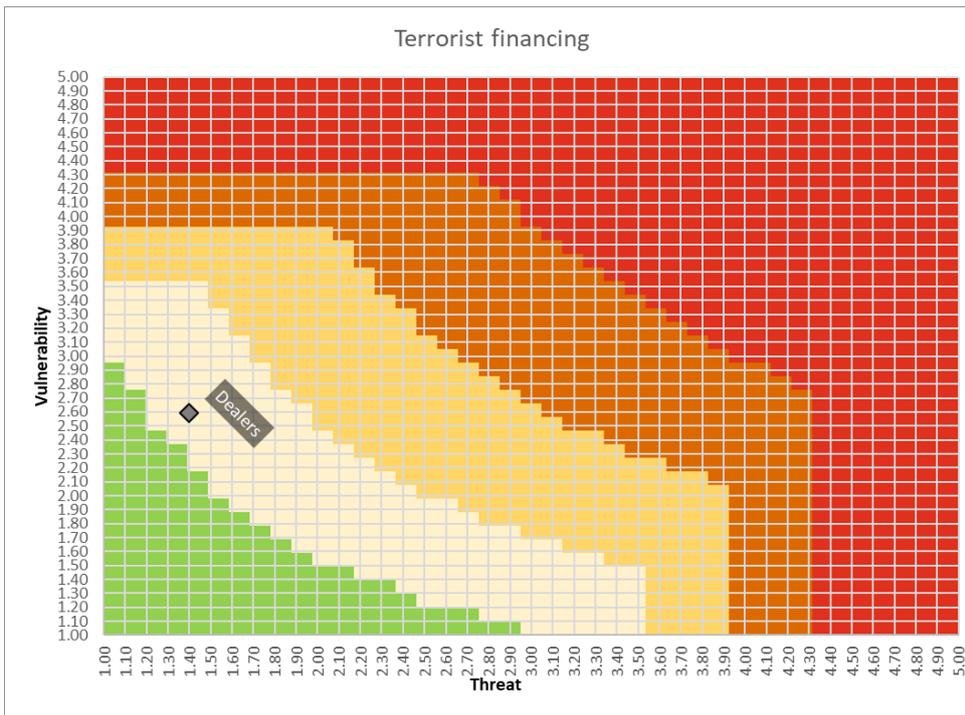
One of the control measures for transactions concluded by dealers is the financial system which has strengthened the control of funds moving between accounts (background and content of transactions) due to large-scale money laundering scandals which have struck Estonia. This placed greater expectations on dealers to know their customers and describe the content of transactions to their home banks and other business partners.

From the point of view of supervision, more vulnerable aspects include the lack of supervisory resources due to most resources as of today being allocated to activities related to activity licences (issue, inspections, and follow-up inspections).

As for dealers, the weak aspects of the application of due diligence measures include unrecognised risks related to the field, insufficient monitoring systems, or a lack of skill to use the existing publicly available data; lack of awareness of risks related to money laundering and terrorist financing, demonstrated by the management itself as well as their employees. Both the trustworthiness of the data in the register of beneficial owners and access to information about politically exposed persons can be considered insufficient, both nationally and internationally. This aspect requires a solution at the national level. There are many market participants in the dealers' sector who are not subjects according to law, however, they also should acquire general knowledge about the threats and risks of money laundering and terrorist financing. A nationwide common approach is necessary, either via umbrella organisations or as a public service IT-solution.

The risk level of terrorist financing in the dealers' sector in the state is in the middle of other sectors and at a below average rating. Therefore, dealers' vulnerability for money laundering may be considered acceptable, but there are market participants for whom an increased awareness of prevention of money laundering is necessary. At the same time, some market participants have room to grow in order to enhance their capability to become even higher in quality, to ensure clearer transactions, and to enable to accurately and adequately evaluate their customers or business partners.

**Figure 16.** Heat map of the terrorist financing risk level in the dealers' sector.



**Summary**

The risk level in the sector from the aspect of terrorist financing is **below average** which means that it is necessary to accept the risk and its consequences as is and there is no need for the application of specific measures. Simplified due diligence measures may be applied in the sector.

**9.5.6. Risk management strategy**

**9.5.6.1. Risk mitigating measures at the state level**

Based on the results of the risk assessment, the following proposals are made to improve the situation at the state level:

- Data from the national registers that is needed for the application of due diligence measures should be provided to the obliged entities free of charge or on more favourable terms;
- Provision of sector-specific guidelines to the market participants (provided by the FIU).

**9.5.6.2. Risk mitigating measures at the level of obliged entities**

Based on the results of the risk assessment, the following proposals are made to improve the situation at the obliged entities level:

- Raising sectoral awareness through training and roundtables provided by the supervisory authorities (FIU);
- Providing training for the employees of companies through the FIU and umbrella organisations (Estonian Chamber of Commerce and Industry, Estonian Vehicle Dealers and Services Association, etc.).