## Non-Restricted Version:

# The Findings of the ML National Risk Assessment: The Financial System


## 2017

# Table of Contents

# Introduction

The FATF (Financial Action Task Force), the organization leading the international fight against money laundering and terror financing, has been diligently working since its establishment on adopting and implementing measures that will prevent the abuse of the financial system for money laundering. According to the international standards set forth by the organization, member countries are required to identify, assess and understand the specific and unique risks facing them concerning money laundering and terror financing based on the financial, demographic and socio-economic characteristics in their countries.

In accordance with the international recommendations, the State of Israel has conducted a national risk assessment of the financial system in Israel, in order to map the fields of financial activity that create money laundering risks, to understand the vulnerabilities that enable their existence, and to examine appropriate control measures. The risk assessment, led by the Israel Money Laundering and Terror Financing Prohibition Authority (hereinafter: "IMPA"), was carried out by each of the financial supervisors with respect to the sector supervised by it, with the participation of the private sector.

The risk assessment is intended to assist the public and private sectors in identifying the risks of money laundering in the country, and to understand the potential risks of these phenomena to the financial system. In addition, the risk assessment is intended to serve as a basis for setting policies and priorities in the prohibition of money laundering and terror financing prohibition domain, for applying of a risk based approach and for allocating resources efficiently.

The risk assessment for the financial system addresses the following financial institutions:

1. The banking system.
2. Stock Exchange Members and securities trading field.
3. Portfolio Managers.
4. Insurance companies and provident funds.
5. The Postal Bank.
6. Money Services Business (hereinafter: "MSB's")

In each sector, financial activities, categories of customers and activity patterns that constitute risks within that sector were identified. Each risk was characterized and rated according to the scope of threat it poses and the vulnerabilities in respect to it.

This risk assessment accompanies the ML NRA, by identifying and assessing the specific risks for each one of the financial sectors, in accordance with its characteristics and the services it provides to its customers.

Below shall be specified the sectorial risk assessments conducted by the Banking Supervision, the Securities Authority (hereinafter: "ISA") the Capital Market, Insurance and Savings Authority (hereinafter: "CMISA"), the Commissioner of the Postal Bank, and the MSB's Supervision Unit.

# The Banking System

The banking system offers a wide range of products and services designed to enable high-quality and advanced banking services for business and private customers.

While most of the customers use products and services for their intended purposes, there are entities seeking "opportunities" to abuse them for money laundering and terror financing.

The banking system mitigates well with the exposure to the risks of money laundering and terror financing by implementing quality controls that ensure the implementation of the money laundering and terror financing instructions, as well as effective measures for tracking, monitoring and risk management of such, whilst considering all of the risk factors in this context.

The banking system's risk assessment was conducted with the full cooperation of the sector and is based on the comprehensive processes and the vast experience accumulated by the Banking Supervision. As part of the process, the banking corporations were asked to answer questionnaires regarding the risks they believe are inherent in the banking system.

The banking system and the Banking Supervision reviewed, mapped and assessed the main money laundering and terror financing risks that are relevant to the banking system, as follows:

- **Money Service Business**

Within the MSB's sector, there are entities operating as financial institutions, providing a wide range of services that include, *inter alia*, checks discounting, foreign currency services and provision of non-bank loans. In light of the aforementioned, the threat posed by this activity is assessed e at a high level.

The mitigation measures include, an instruction on periodic reporting to the Banking Supervision, which must include information regarding on the activity of high-risk customers. In addition, the banking corporations are required, *inter alia*, to monitor international transfers and cash-intensive activity and to report to IMPA, in accordance with the provisions of the law.

**The level of the risk of money laundering and terror financing posed to the banking system due to the activity of MSB's is assessed as high.**

- **Associations and Non-Profit Organizations**

Associations (*Amutot*) and non-profit organizations (hereinafter: "NPO's") are characterized by extensive use of cash, international activities, providing loans and receiving deposits, anonymous donors and high financial turnover. These characteristics are risk factors for money laundering and terror financing. The level of threat posed by their activity is assessed as moderate-high.

The mitigation measures include an instruction on periodic reporting to the Banking Supervision, which must include information regarding the activity of high-risk customers. In addition, the banking corporations are required, *inter alia*, to monitor international transfers and cash intensive activity and report IMPA, in accordance with the provisions of the law.

**The level of the risk of money laundering and terror financing posed to the banking system due to the activity of associations and NPOs is assessed as high.**

- **Cash**

Cash is an anonymous means of payment, which enables disguising illegitimate activities within the banking system. Due to the extensive use of cash and the ease with which it can be transferred, the risk is assessed at a high level.

The ability of the banking system to cope and enforce this risk is derived from the provisions of the law, including the Prohibition on Money Laundering Order, which imposes on banking corporations reporting obligations for carrying out cash transactions over the threshold set forth in the order. It should be noted that the banking corporations have developed mechanized rules and laws for tracking cash transactions even below the thresholds required under the provisions of the order. In addition, in accordance with the on reporting obligations to the Banking Supervision, the banking corporations are required to report information regarding the activity of high-risk customers. An understanding is seen in respect of the risks of money laundering and terror financing which are carried out with cash. In light of this and of the supervision and monitoring obligations applied concerning this threat, the vulnerabilities within the cash activity are assessed at a moderate level.

**The level of the risk of money laundering and terror financing posed to the banking system due to cash activity is assessed as moderate-high.**

- **Private Banking**

Private banking services are provided to wealthy individuals - foreign residents and Israelis, in Israel and around the world, In view of the potential risk and its implications, the threat posed by this activity is assessed as high.

The vulnerabilities of private banking services exist in cross-borders activity, and in the need to take measures to reduce risk arising from this activity. An additional vulnerability is the lack of an organized list of tax havens, which is required due to the common activity pattern of money laundering which is carried out through offshore corporations.

The mitigation measures include, *inter alia*, the tracking international transfers, the reporting obligation to IMPA in accordance with the provisions of the law, the requirement of periodic reporting to the Banking Supervision regarding activities of high-risk customers; and guidelines aimed to reduce the exposure of banking corporations to cross-borders activities. In light of the aforementioned, the ability to deal with the abuse potential of the private banking activity is assessed at a moderate level.

**The level of the risk of money laundering and terror financing posed to the banking system due to the activity of private banking is assessed as moderate-high.**

- **The Diamond Industry**

The diamond industry is supervised by the Ministry of Economy, which provides licenses to engage in this activity, which by its nature is exposed to the risks of money laundering and terror financing, and at times may be abused.

Money laundering through legitimate activity in the diamond industry is being investigated and handled by the enforcement authorities, which recently invested great efforts in minimizing the risks inherent in this activity. In addition, a periodic reporting obligation to the Banking Supervision, include reporting information regarding the activity of high-risk customers. Moreover, the banking corporations are required to implement quality controls, *inter alia* , tracking international transfers and reporting to IMPA in accordance with the provisions of the law.

**The risk level of money laundering and terror financing posed to the banking system due to such activity is assessed at this stage as moderate-high.** At the same time, we expect that the risk minimization measures conducted by the enforcement authorities will soon change the risk level.

- **International Transfers**

International transfers pose a risk to the banking system especially in situations where the bank transfer is made to / from an account located in a country defined as a country at risk; in situations where the source of the funds or their destination is countries that are known as tax havens, and also in situations where the counter party

to the transaction is not identified by name or account number. The threat posed by such activity to money laundering and terror financing is assessed as high.

The State of Israel does not hold an organized list of countries and territories that are known as tax havens. However, the supervision measures, include, the Prohibition on Money Laundering Order, which imposes "automatic" reporting obligations on certain funds transfers between Israel and countries abroad, and of certain funds transfers between Israel and a high-risk country. The ability to cope and enforce the risk is assessed at a moderate level.

The banking corporations have developed mechanized rules and laws for identifying international transfers, even under the thresholds set out in the provisions of the law. Efforts have been made to identify cases in which attempts have been made for bypassing the reporting obligation on several levels, including making the tracking and monitoring systems stricter.

**The risk level of money laundering and terror financing posed to the banking system due to such activity is assessed as moderate-high.**

- **Managing Accounts for Another through Complex Incorporation Structures**

In such cases, it is difficult to track the chain of holdings, the controlling shareholder and the final beneficiaries. The difficulty increases in cases where the corporations are registered in tax haven countries and raise capital originated abroad.

**The risk level of money laundering and terror financing posed to the banking system due to such activity is assessed as moderate-high.**

- **Offshore Corporations**

Offshore corporations are companies registered in countries and territories known to facilitate on corporate law and tax law. These areas are characterized by a low level of enforcement that, which at times, enables carrying out operations in various manners, as well as in facilitating procedures for the identification and registration of the controlling shareholders and beneficiaries. The level of threat posed by activity in offshore corporations' accounts is assessed as moderate-high

The banking system as a whole is aware of the exposure to the risks inherent in such corporations.

**The risk level of money laundering and terror financing posed to the banking system due to the activity in offshore corporations' accounts is assessed as moderate-high.**

- **Politically Exposed Persons**

The State of Israel has adopted the international standards for the identification of public figures. Due to the concern of public figures will abuse the banking system for covering acts of corruption and bribery, the level of the threat h is assessed as moderate-high.

The provisions of the law apply to the banking system include, *inter alia*, provisions requiring enhanced identification and monitoring the activity of foreign PEPs. They are defined as being high-risk customers, and, due to their activities, increased monitoring measures are exercised, including built-in rules within the mechanized system for identifying patterns of unusual activity. Thus, the mitigation measures are assessed as moderate-high.

**The risk level of money laundering and terror financing posed to the banking system due to the activity of public figures is assessed as moderate - high.**

- **Internet Activities and Digital Currencies**

In recent years internet activity has become increasingly diversified. Trade has also shifted in this context to digital trade operating using virtual currencies. These Currencies are not legal tender of any country. The threat level posed by this activity is assessed as moderate-high.

In accordance with the reporting obligations, banking corporations are required to report to the Banking Supervision information regarding the activity of high-risk customers.

**The risk level of money laundering and terror financing posed to the banking system due to this activity is assessed as moderate-high.**

- **Correspondent Banking**

Correspondent banking is used for international transfers. The correspondent bank (which provides services to another bank abroad) is required to examine, be acquainted with and understand the nature of the business of its respondent banks, obtain information on their business activity, the location of their businesses, and the efforts they take to prevent money laundering and terror financing. In addition, it is forbidden maintain relations with a banking institution that is not supervised in respect to the prohibition of money laundering and terror financing. The threat level posed by such activities is assessed as moderate.

**The risk level of money laundering and terror financing posed to the banking system due to the activity of correspondent banking is assessed as moderate.**

- **Trust Accounts**

In these accounts, relations are maintained between a number of entities, including the trustee and the beneficiary. Managing of an account by a third party in favor of another is one of the risk factors for money laundering and terror financing.

**The risk level of money laundering and terror financing posed to the banking system due to the activity in trust accounts is assessed as moderate.**

- **The Arms Industry**

The arms industry includes, *inter alia*, defense industries and security service providers. The Ministry of Defense supervises the activity of the arms industry and issues detailed licenses for trading in weapons including the types of products and the target markets. The arms industry is inherently exposed to the risks of money laundering and terror financing. The threat posed by the activities of the arms industry is assessed at a moderate level.

The offense of illegal trade in arms is listed in the predicate offenses' list under the Prohibition on Money Laundering Law. In accordance with the reporting obligation, banking corporations are required to report information regarding the activity of high-risk customers to the Banking Supervision.

**The risk level of money laundering and terror financing posed to the banking system due to this activity is assessed as moderate.**

- **Real Estate Transactions**

In recent years, real estate activity has boomed and accordingly, there has been a significant increase in the real estate prices in Israel. The risk of money laundering and terror financing is embedded in real estate transactions characterized, *inter alia*, by the extensive use of cash, international activities and complex transactions.

**The level of the risk of money laundering and terror financing posed to the banking system due to real estate transactions of such nature is assessed as moderate.**

# Stock Exchange Members and Securities Trading

In general, the sector of Non-Bank Stock Exchange Members[1] (hereinafter: " Stock Exchange Member") is not characterized as a high level of risk of money laundering and terror financing at the national level, both in view of the relative size of the sector, and because most Stock Exchange Members do not allow transfers of cash. Additionally, third party transfers are not common, and when they are carried out they are subjected to the close supervision of the Stock Exchange Members. The main risk in the activity of Stock Exchange Members relates to the layering phase of money laundering and the main typologies related to exploitation of trade and conducting artificial transactions designed to disguise money transfers between the parties. In this context, it should be noted that securities trading is not characterized as a high level of risk for money laundering and terror financing due to public documentation of the security's ownership, as well as the high level of monitoring the trade and the enforcement capabilities of the ISA. It should be noted that on 24/06/2016 the Prohibition on Money Laundering Order came into force, which applies reporting and monitoring obligations within the domain of the prohibition on money laundering and terror financing on licensed Trading Platforms, and the ISA was also authorized to supervise the implementation of the obligations under this Order as well.

Below shall be listed the main risks identified in respect of Stock Exchange Members activity and the Trading Platforms sector:

- **Trading Platforms**

On 26/5/2015 Amendment No. 42 of the Securities Law came into force, applying a licensing and supervision regime to the Trading Platforms sector, and 6 licenses had been issued[2] by the ISA during September and November of that year. Along with

[1] Trading on the Stock Exchange is carried out by the stock exchange members. The ISA monitors the non-bank stock exchange members in respect of prohibition of money laundering and terror financing. Stock exchange members that are banking corporations are supervised by the Banking Supervision in respect of prohibition of money laundering and terror financing.

[2] Trading Platforms are computerized systems through which one trades financial instruments with his customers into his personal account, as well as computerized systems that enable a customer to trade in such systems. A financial instrument is defined, *inter alia*, as an agreement or arrangement derived from currency exchange rates, shares and commodities. .

Among the financial instruments offered to customers by some of the companies that applied for a license, were also companies offering binary options. On 21/3/16 the ISA announced its decision not to approve trading in binary options by licensed trading platforms. This is due to the complexity of binary options and the difficulty in pricing them on the one hand, and absence of multi-party trade that enables the creation of a market price, on the other hand. The ISA noted in its decision that due to the characteristics of binary options, as well as the characteristics of the trading platforms, the service is essentially similar to gambling. According to the decision, the license applications of

this supervision regime in accordance with the Securities Law, license holders for trading platforms were subjected to to prohibition of money laundering and terror financing obligations, in the same manner as Stock Exchange Members and other financial entities. The risk in this section addresses trading platforms that are not subject to the licensing requirements, due to the fact that according to the territorial applicability of the Securities Law, trading platforms operating from Israel, in a full or partial manner, and all of their customers are foreigners, so that they do not address the Israeli public, do not require a license. The activity of Trading Platforms includes, *inter alia*, financial transfers, including international transfers, vis-a-vis customers outside of Israel. As a result, the threat in the trading platforms sector is rated at a high level.

In light of the aforementioned and the indications regarding the scope of this phenomenon, **the risk level in this area is rated at a moderate-high** level.

- **Non-Supervised Broker-Dealers**

Broker-dealers activity does not require a license in Israel and is not subject to the reporting regime to IMPA, unless the activity falls into one of the existing regulation categories in respect to stock exchange members and banks. As part of the risk assessment, separate reference was made to two existing activities, as specified below:

- **Provision of Brokerage Services by a non-supervised entity**: In this scheme, a broker-dealer trades securities for customers through the nostro account and conducts the transactions with the customers' accounts at a Stock Exchange Member or bank. In the case of transactions in foreign securities, the activity will usually be carried out dealing with a broker-dealer subjected to supervision in his respective country. As the broker-dealer is not supervised and is not required to report to IMPA, it is likely that they will not carry out established procedures for assessing the risk of money laundering and terror financing in their activity. The vulnerability is, as noted, the lack of regulation in this field.

  Among the risk mitigation factors, it should be noted that the stock exchange member is obligated to implement identification procedures, KYC process and reporting to IMPA and in case of foreign securities, vis-à-vis a supervised broker-dealer.

  In light of the aforementioned **the risk is rated at a moderate level.**

companies offering trade in binary options were denied, unless the companies announced that they had stopped offering binary options.

- **Provision of brokerage and money transfer services by a non-supervised entity**: In this category, a broker-dealer who trades in securities provides additional services. Unlike the previous activity outline, this outline of activity is not limited only to securities brokerage transactions, and also includes activity of financial transfers, including international transfers.

  Among the risk mitigation factors, it should be noted that the stock exchange member is obligated to implement identification procedures, KYC process and reporting to IMPA and in case of foreign securities, vis-à-vis a supervised broker-dealer.

  In light of the aforementioned, and in lack of indications of widespread scope of this phenomenon, **the risk is rated at a moderate level.**

❖ **Domestic Politically Exposed Persons (PEPs)**

The international standards that apply to domestic PEPs are similar to those that apply to foreign PEPs. Despite the perception of this threat as significant, the data received by the ISA from the Stock Exchange Member shows that the scope of activity of local public figures within Stock Exchange Members accounts is limited. However, due to the lack of clear definition of domestic PEPs under the Stock Exchange Members Order, this data does not necessarily fully reflect the extent of this customer's activity with the Stock Exchange Members. In weighting all of the aforementioned, this threat was rated at a moderate level.

Vulnerabilities - at the time the risk assessment was carried out, the international standards were not adopted in the context of the domestic PEPs in the Stock Exchange Members Order. In light of the aforementioned, **the risk is rated at a moderate level.**

❖ **Foreign PEPs**

In accordance with the international standards, foreign public figures are considered to be a high-risk for corruption and money laundering, as they may take advantage of their status and influence for their personal benefit. According to the data of the Israel Money Laundering and Terror Financing Prohibition Authority, the scope of this threat is not high, and as the information received by the ISA from Stock Exchange Members shows, the scope is limited. In light of the limited scopes of the phenomenon in general, and with Stock Exchange Members in particular, the threat in this field is rated at a moderate-low level.

Risk mitigating factors and monitoring measures - the Stock Exchange Members Order requires that when a customer is defined as foreign public figure, the approval

of an office holder is required; including increased monitoring the activity in his accounts. IMPA has published guidelines and clarifications document regarding prohibition of money laundering originating from corruption and bribery of foreign public figures. Considering the limited scope of this phenomenon, the monitoring measures and the estimates that the likelihood of the phenomenon to increase is low, the risk is classified at a moderate-low level.

- **Providing Brokerage Services without Opening an Account**

Some Stock Exchange Members provide securities brokerage services through their nostro account without opening an account for the recipient of the service, and thus, without conducting identification procedures and KYC process, in accordance with the requirements of the Prohibition of Money Laundering Order that applies to Stock Exchange Members (hereinafter: the "Stock Exchange Member**s Order**"). It should be noted that even in such cases, NBFI are required to report suspicious and unusual transactions.

Among the risk mitigating factors, it should be noted that usually the activity is carried out for supervised entities that are well known to Stock Exchange Members. In addition, in accordance with order, Stock Exchange Members are required to report suspicious and unusual transactions also where an account is not opened for the recipient of the service and therefore setting forth tools and procedures for dealing with the risk. Additionally, the securities commerce is carried out in dealing with the recipient of the service account with another stock exchange member, who carries out a identification and KYC processes. In the case of foreign securities, it is carried out in dealing with the recipient of the service account in front supervised broker, in respect of money laundering in his country.

In light of the aforementioned and considering the risk mitigating factors described above, **the risk is rated at a moderate-low level.**

- **Private Issuances**

In a private issuance, a company traded on the stock exchange issues securities to a certain number of investors and may obtain direct proceeds other than through a stock exchange member. The traded companies are not included in the list of entities subjected to a reporting regime to the IMPA. In light of this and considering the relatively low volume of the phenomenon, the threat posed by it is rated at being of a moderate-low level.

Among the risk-mitigating factors, it should be noted that the registration of the ownership of the traded securities and the companies' obligation to report the issuances through an electronic reporting system to the ISA, the stock exchange and the public, enables tracking the ownership of the securities and the date of change of

ownership, which reduces the motivation for committing money laundering offenses through securities trade.

In light of the aforementioned **the risk inherent in this phenomenon is rated at a moderate-low level.**

- **Securities in Kind**

In some of the corporations traded on the Stock Exchange, in addition to the securities registered with the Stock Exchange through a Nominee Company, there are also securities registered with the company's shareholders registrar not through a nominee company. Up until the securities are deposited with the Stock Exchange, the ownership of such may be transferred outside the Stock Exchange in accordance with the companies' regulations. Due to the fact that prior to their deposit in the Stock Exchange the supervised stock exchange members are not involved in the process of transferring the ownership and proceeds from the securities, this asset can be compared to other assets, that are not subjected to supervision and monitoring in respect of money laundering.

It should be noted that among the risk-mitigating factors and monitoring measures, the registration of ownership of securities in kind enables tracking the ownership of the relevant securities and the date of change of ownership, which reduces the motivation for committing money laundering offenses through trade in securities. Additionally, in accordance with the Amendment of the Securities Law, the use of securities in kind has been reduced so that in new issuances it is required to register the securities through a nominee company, subject to a number of exceptions.

In light of the aforementioned **the risk in this field is rated at a moderate-low level.**

- **Money Service Business**

Accounts of customers that are defined as MSB's are exposed to money laundering risks, *inter alia* due to the ease of transferring funds without the need for account activity, and the speed in which transactions may be carried out. According to the data, the volume of the Stock Exchange Members for customers defined as being MSB is low.

In view of the above, and in light of the entry into force of the Amendment of the Supervision of Financial Services Law (Regulated Financial Services) 5776 - 2016, the **risk is rated as a moderate-low level.**

- **Lack of a Mechanism to Transfer Information Regarding the Identification of an Account Owner Between Financial Entities**

Due to the difficulty in identifying the customer face-to-face, and considering the global trends in this field, the ISA initiated alleviations for the manner of identifying low-risk customers, which are managed in a closed system, where all of the funds in the account are returned to the original account from which such have been received and managed at a banking corporation or another Stock Exchange Member.

However, in light of failure to transfer the full information regarding the identity of the account owner by the financial institutions, the Stock Exchange Member have to rely on the identification documents provided by the customer, a fact which undermines the quality of identification. In order to reduce the risk, the ISA published additional instructions setting forth identification and verification obligations for such cases. At the same time, the process becomes complicated and creates unwanted barriers.

Weighting the data, **the risk level is rated at a moderate-low level.**

- **International Transfers**

International transfers pose a risk of money laundering especially in situations where the transfer is made to/from an account located in a country that is defined as a country at risk, situations where the source of the funds or their destination are countries that are known to be tax havens, and also in cases where the counter party of the transfer is not identified by name or account number. The data indicates that the volume of international transfers carried out by Stock Exchange Members is not very high, and thus, the level of threat posed is rated at a moderate level.

The main vulnerabilities include *inter alia* the obligation to reporting international transfers over 1 million NIS. Among the risk mitigation factors and monitoring measures, it should be noted that Stock Exchange Members monitor the transactions in their customers' accounts.

In light of the aforementioned, **the risk is rated at a moderate-low level.**

- **Associations, Free-loan Funds and NPO**

This field is characterized by cash-intensive activity; the ability to disguise funds transfers as donations; international activity and anonymous donors, which make it difficult to track the funds trail and enable the integration of prohibited property in the entities' activity. According to the data, the scope of use made by these entities in the services of Stock Exchange Member is limited.

Vulnerabilities - third parties for whom the funds are held are identified as beneficiaries only and thus the Stock Exchange Member is unable to link activities carried out in the account to the final beneficiary. Among the risk mitigating factors

and monitoring measures, it should be noted that in accordance with the guidelines of the ISA, such entities are an indication of accounts that might be at high risk for money laundering and terror financing.

In light of the aforementioned, **the risk is rated at a moderate - low level.**

- **Activities with Derivatives**

Activities with derivatives where the tradability level is low may be exploited for money laundering by performing artificial transactions for the purpose of disguising money transfers between parties. According to the data, the volume of activity of Stock Exchange Members in derivatives is relatively small.

Among the risk mitigating factors and monitoring measures, it should be noted that the Stock Exchange Regulations include a prohibition on carrying out derivative transactions outside of the Stock Exchange, a fact that significantly reduces the risk level of the activity. In addition, Stock Exchange Members supervise the activity in their customer's accounts, and additionally, the ISA monitors trade and enforces in cases relating to committing securities offenses.

In light of the aforementioned**, the risk is rated at a low level.**

- **Trade in Low Negotiability Securities**

Low negotiability securities are characterized by low trading volumes, and therefore, trading in such may be exploited for money laundering purposes by performing artificial transactions, for the purpose of disguising money transfers between parties.

Among the risk mitigating factors and monitoring measures it should be noted that Stock Exchange Members monitor the activity in their customers' accounts, and additionally, the ISA monitors trade and enforces in cases relating to committing securities offenses.

In light of the aforementioned**, the risk is rated at a low level.**

- **Tax Shelters and Offshore Corporations**

The use of tax havens and offshore countries may be exploited for the purposes of money laundering and tax evasion, both by international transfers as well as by the customers of Stock Exchange Members which are corporations registered in these locations. Often, the money laundering prohibition regime in these locations is not sufficient and it is difficult to trace the origin or destination of the funds, or the control over the corporation. Data obtained by the ISA indicates that the scope of the

relevant activity by Stock Exchange Members is low, and therefore the threat is rated at a low level.

Among the risk mitigating factors and monitoring measures, it should be noted that in accordance with the guidelines of the ISA, registration of a corporation in a tax haven country is an indication of accounts that might be at high risk for money laundering and terror financing. In addition, the Enforcement of Tax Collection and Strengthening of Enforcement Law (Measures for the Enforcement of Tax Payments and Alerting of Money Laundering), 5775 - 2015, which sets forth severe tax offenses as being predicate offenses under the Prohibition on Money Laundering Law, came into force in October 2016.

In light of the aforementioned and noting the expectation that use of companies and accounts in these countries will decrease due to international activity in respect of the matter, the **risk posed by these activities is rated at a low level.**

- **Trusts**

The trusts sector is not subjected to a reporting regime regarding money laundering except in situations where the activity falls within areas regulated under the law, such as lawyers and accountants. Trust accounts are convenient place to disguise the true identity of beneficiaries, *inter alia* because in Israel there is no registry that includes all of the trusts, and thus the information regarding beneficiaries cannot be verified. In light of the severity of the threat, the field is rated at a moderate level.

Among the risk mitigating factors and monitoring measures, it should be noted that most of the activity in trusts accounts with Stock Exchange Members is mainly conducted in bonus shares accounts. In such activity, the trustees are entities closely supervised by the Tax Authority.

In light of the aforementioned, **the risk is rated at a low level.**

- **Cash**

Data of the Israel Money Laundering and Terror Financing Prohibition Authority indicates that cash is the main pattern for money laundering. Its use is anonymous and makes it difficult to trace the money route and its origin *inter alia*, by using techniques for avoiding the reporting obligation, such as splitting the deposits amounts. Although this is a severe threat, data received by the ISA indicates that the scope of the phenomenon among the Stock Exchange Members is low, and therefore, the threat in this field is rated at a moderate- low level.

Vulnerabilities - with regard to cash deposits made into an account managed in Stock Exchange Members by a bank, the Money Laundering Prohibition Order that applies

to the banking corporations, grants an exemption to Stock Exchange Members from making a declaration of a beneficiary in its account and the bank is not required to conduct an identification and KYC processes for low cash transaction. At the same time, the Stock Exchange Members monitor the activity carried out, and if necessary reports to IMPA. In light of the aforementioned and the assessment that the scope of use of cash will be reduced, **the risk in this field is rated at a low level.**

- **Diamonds**

The unique characteristics of diamonds are convenient grounds for money laundering and terror financing activity. However, the data indicates that the volume of activity of those engaged in the field is low among Stock Exchange Members, and therefore the threat in the field is rated at a low level.

The vulnerabilities refer to the absence of reporting of international transfers for import or export. In addition, the Money Laundering and Terror Financing Prohibition Order that applies to diamond dealers, only applies to cash transactions, and applies only to the seller.

Considering that the volume of activity of those engaging in the field is low among NBFI, **the risk is rated at a low level.**

## Portfolio Managers

The activity outline within which a portfolio manager operates in Israel is unique. He is required to obtain power of attorney from the customer in order to operate in his account, and is allowed to conduct purchases and sales transactions in securities only. The portfolio manager does not keep or receive funds or assets from the customer, and cannot transfer assets from the customer's account. In addition, the portfolio manager operates in a customer's account, for which identification and verifications procedures have already been taken. Thus, it can be said that the portfolio manager is a safety and monitoring networking.

Below shall be listed the main risks identified regarding portfolio managers' activity.

- **Initiated Requests of the Customer Made to a Portfolio Manager**

In cases of initiated requests, the portfolio manager is unable to exercise independent discretion. Outwardly, the account is managed by them, making it difficult to track the customer's activity. During the risk assessment, it had been found that such is a rare money laundering phenomenon. Initiated actions by customers are not common, and the portfolio managers avoid accepting instructions from customers, for business and operational reasons. In light of this data, the threat is rated at a moderate level.

There is no prohibition under the law regarding the transfer of initiated requests to the portfolio manager concerning conducting actions in an account managed by the customer. However, at the same time, this activity is regularly monitored by the portfolio managers. In addition, the ISA is authorized to impose administrative sanctions for failure to conduct regular monitoring and to transmit reports regarding cases that raise concern of a threat. In light of so, and in lack of findings to prove the existence of a threat as aforementioned in the portfolio managers activity in the unique course of activity within the Israeli market, **the risk is rated at a low level.**

- **Management of Investment Portfolios in the Absence of Mandatory Licensing**

The Consulting Law sets forth a list of occupations that do not require a license. Exemption from licensing requirements for the provision of investment portfolio management services will be obtained in two cases: the first, management of up to five customers during a calendar year; the second case deals with granting an exemption to a competent customer.

The ability to engage in portfolio management without a license poses difficulties to the effectiveness of the supervision and enforcement actions. However, there little evidence that these exemptions pose a threat in terms of money laundering. In light of

the aforementioned, and considering the unique activity of portfolio managers, the threat posed by their activity is rated at a moderate level.

In general, the Authority does not monitor activity that are not supposed to be supervised by it, unless there is information that raises real suspicion that an activity expected to be supervised where it is not, or where an activity requiring licensing and monitoring is conducted without a license. It should be noted that the Authority is unable to supervise and monitor entities that engage in the field in the absence of licensing as aforementioned, as such entities are not subjected to reporting or registration obligations

It is important to note that that the enforcement authorities' position is that the obligations set forth in the Portfolio Managers Order apply to all of those engaged in portfolio management, whether or not they are licensed. In light of the aforementioned, including the fact that the volume of activity through an exemption is low and there are is no evidence of a real concern regarding the money laundering aspect, **the risk is rated at a moderate - low level.**

- **Entities Registered with a Portfolio Manager are Not Identical to Those Registered for the Customer's account in the Bank or Stock Exchange Members**

The account owner in a bank or Stock Exchange Member is the account owner at the portfolio manager, since the portfolio manager operates in his account in the bank or Stock Exchange Member However, there may be a situation in which there is an authorized representative or an additional beneficiary appearing at the portfolio manager, but not in the bank or Stock Exchange Member. This scenario has two risks: first, control of the customer's account by adding an entity in the managed account that is not known to the bank or stock exchange member; second, concern of identity theft. Regarding the first risk, it is difficult to estimate the number of accounts that are managed and in which there is a risk of money laundering. As for the second risk, the phenomenon is not common as means for money laundering, and there is no data regarding this pattern of activity. Thus, the threat is rated as being at a moderate level.

The most significant vulnerability relates to the absence of an obligation to identify the entities registered with the portfolio manager and compare them with those existing in the customer's account. The customer is not obligated to declare the entities in the account to the portfolio manager on, apart from a declaration of a beneficiary in the account. Therefore the portfolio manager is unable to know whether there is a difference between the power of attorney in the managed account and that in the bank or Stock Exchange Member account and vice versa. The Authority conducts inspections with the portfolio managers, during which, , the validity and propriety of beneficiary statements, unusual entities in the managed accounts, the supervision performed in the account and implementation of the obligation to submit unusual

reports are examined. Administrative sanctions may be imposed in respect of a violation of any of the aforementioned obligations. Additionally, the portfolio manager is required to conduct a procedure of verification identification process for the power of attorney, including ongoing monitoring of the managed accounts, and *inter alia*, the identification of unusual entities. In light of the aforementioned and in lack of evidence indicating that this matter causes direct damage and adversely affects the portfolio manager's activity and as there is no expectation of long-term damage, **the risk is rated at a moderate level.**

- **Trade in Low Negotiability Securities**

Trade in low negotiability securities by a portfolio manager requires a customer interested in committing criminal activity to change the price of security, to be involved in the management of the portfolio by transmitting initiated requests for transactions in low negotiability securities. Thus the existence of a portfolio manager in the middle reduces the threat. There is no documentation that there is a threat posed in terms of money laundering and terror financing. Therefore, the threat is rated at a low level.

The securities trading fraud offense is listed in the predicate offenses' list under the Prohibition on Money Laundering Law. The authority monitors trade and opens investigations following suspicion of fraudulent trading in securities. Due to the risk of money laundering, as a policy, most portfolio managers do not accept requests for conducting transaction in securities with low negotiability according to a customer demand, but only according to the decision of the portfolio manager in the company. In addition, the Authority, in collaboration with the Stock Exchange, has established a "list of low-tradable securities" which is updated twice a year in order to reduce the possibilities of manipulation in these securities. In light of the low volume of the phenomenon and the activity pattern, through portfolio managers, **the risk is rated at a low level.**

## Institutional Entities

The CMISA is responsible for the regulation and supervision of the financial services sector in Israel, including insurance companies, pension fund management companies managing pension funds and provident funds management companies (hereinafter - "**Institutional Entities**"). The Authority is headed by the Commissioner of the Capital, Insurance and Savings Market. The functions of Authority are to protect the interests of policyholders, members and customers of the supervised entities; ensuring the stability and proper management of the supervised entities; promoting competition within the capital, insurance and savings market and the financial system, as well as encouraging technological and business innovation.

Below shall be listed the main risks identified regarding institutional entities' activities.

- **Loans to Members and Policy holders**

The threat in this area is characterized by taking loans against funds accumulated in an account or policy around the time of the deposit (which generally lacks financial sense), as well as the involvement of a third party who does not receive the service. Due to the low volume of activity in this field, the threat is rated at a low level.

The vulnerabilities are the standard reporting threshold set forth under the Order, which stands at a sum exceeding one million NIS, and the absence of the obligation to conduct KYC process. On the other hand, the mitigation measures include, inter *alia*, the use of information systems for the purpose of detecting and monitoring risks, conducting inspections and imposing sanctions. Therefore, **the risk is rated at a low level.**

- **Deposits in Investment Policies**

There are a number of symptoms characterizing the threat in this area, which are expressed in withdrawing funds from an investment policy around the time of deposit; third party involvement that does not receive the service and contracting in a large number of investment policies in small sums. In recent years this field has developed and is currently estimated at 25 billion NIS. Thus, the threat posed in this field is rated at a moderate level. The vulnerabilities derive from the fact that investment policies may be withdrawn at any time, rather than only upon the time of retirement, and that the Orders do not regulate a full KYC process. However, for the purpose of disclosure and monitoring risks, the institution entity's information systems and the order that determines reporting obligations are used. . Additionally, there are inspections conducted by the regulator who is authorized to impose sanctions in appropriate cases. Thus, **the risk is rated at a moderate level.**

❖ **Deposits or Withdrawals in the Account or Policy**

The threat embedded in this area of activity is expressed by a number of forms: the involvement of a third party that is not the one receiving the service; cash deposits in the bank that raise difficulties in identifying the depositor; deposits and withdrawal before reaching retirement age, in particular their withdrawal around the time of deposit or conducting a large number of deposits into a policy or account in small amounts, the accumulated total of which is high. In light of the fact that the cases described are carried out in a low scale, the threat is rated at a low level. The vulnerability derives from the standard reporting threshold set forth under the Order, and in the absence of the requirement to conduct a full KYC process. However, for the purpose of disclosure and monitoring of risks, the institution entity's information systems and the order that determines reporting obligations are used. . Additionally, there are inspections conducted by the regulator who is authorized to impose sanctions in appropriate cases. Therefore, **the risk is rated at a low level.**

It should be noted that in March 2017 the new Orders of the institutional entities were updated, for the first time since 2001, and are expected to come into force in February 2018. As a result, significant improvements are expected to apply in respect of the money laundering and terror financing regime in this field, *inter alia*, with respect to reporting obligations and KYC process. In accordance with and in light of the mitigation measures, which include disclosure and monitoring operations through use of the institutional entities' information systems as well as the regulator's powers to conduct inspections and impose sanctions where appropriate.

To conclude, **the risk inherent in the activity of institutional entities is rated at a low level.**

# The Postal Bank

The Supervision of the Postal Bank Division was established at the Ministry of Communications upon the transfer of the Postal Bank activity to the Postal Company and revocation of the Postal Bank Law. The Postal Bank engages, *inter alia*, with the management of a payment and collection systems, the purchase and sale of foreign currency, international money transfers, the issuance of pre-paid cards in foreign currency, the distribution of credit and deposits, and the management of checking accounts for private and business customers. The Postal Bank provides its services to the entire public nationwide with approximately 700 postal units scattered throughout the country.

The Postal Bank conducts a comprehensive risk assessment every two years, which includes identification, assessment, monitoring and management of all of the risks identified in its activities, taking into account the Bank's resources and the changing environment in which it operates. Accordingly, an efficient and risk based work plan is formulated, which includes manner of treatment of each of the risks identified.

The Postal Bank is subject, *inter alia*, to the provisions of the Prohibition on Money Laundering Order (Obligation of Identification, Reporting and Keeping Records of the Postal Bank for the Prevention of Money Laundering and Terror Financing), 5771 - 2011 (hereinafter in this chapter - the "Order") as well as the Commissioner's instructions regarding prevention of money laundering and terror financing, risk management at the Postal Bank and the compliance officer (hereinafter in this chapter - the "Instructions")

- **Cash Activity and Transactions of Occasional Customers**

These activities pose a significant threat as such may be carried out through funds originating in predicate offenses, and as casual customer's actions are carried out without use of an account.

The applied mitigation measures require investment of resources, including applying a Know Your Customer process, obtaining documents that support the origins of the funds and the nature of the transaction, in each cash transaction above a certain threshold, as well as conducting an enhanced KYC process for cash-intensive customers and for Money Service Business customers. In addition, the Postal Bank exercises comparison with lists of organizations and individuals who have been designated to be terror activists; exercises monitoring measures and automated modules for detecting activities in sums exceeding a specific threshold; examines the nature and purpose of the transaction; and conducts initiated inspections on compliance with the provisions of the law and the instructions. Additionally, the Postal Bank conducts trainings for the monitoring personnel and service

representatives regarding to obtaining proper supporting documents as to the origin of the funds and the transaction's nature.

In the past year, following the actions of the Postal Bank, there was a significant decrease (approximately 80%) in the use of cash by the Bank's customers and accounts of customers who did not meet the Postal Bank's requirements were closed, including the increased KYC process and the transfer of supporting documents in accordance with the Order and the instructions. In weighting the data, **the risk inherent in use of cash by casual customers is rated at a moderate-high level.**

- **Money Service Business and *'Gemilut Chasadim'* Activitiy**

As stated above, the Postal Bank exercises many operations in order to reduce the threat posed by these entities, and rates their accounts to be of high risk level of money laundering. Additionally, excluding the reporting obligation to the Israel Money Laundering Prohibition Authority, there are additional tools for risk management and monitoring - the Postal Bank directs MSBs to branches designated for them, and conducts an increased KYC process for every MSB. Moreover, the Postal Bank operates mitigation measures and operated automatic modules that identify transactions in excess a specific threshold for the purpose of a comprehensive examination of the customer's activity. In weighting the data, **the risk inherent in this activity is rated at a moderate-high level.**

- **Cross-Borders Activity**

This activity is characterized by opening accounts by foreign customers, as there is concern that in certain cases this activity is carried out in order to avoid paying taxes in the destination countries, and thus there is a built-in risk in these accounts.

In January 2016, the Supervisor of the Postal Bank issued fit & proper management instructions concerning the management of risks arising from cross-border activity of customers, which included a series of essential procedures and steps that must be taken before opening an account for foreign customers. This instruction includes specific obligations for reducing this risk, in addition to the Commissioner's instructions as aforementioned, and therefore the vulnerabilities are rated at a moderate level.

In light of the aforementioned, **the weighted risk is rated at a moderate level.**

- **Frequent Funds Transfers Inside the Country**

The widespread deployment of postal units in Israel enables frequent transfers of cash in short periods of time. This activity embeds the risk of transferring cash originating from predicate offenses, and thus the threat level in this field is rated at a moderate-

low level. The Postal Bank conducts a large number of inspections in respect of the use of these services and, when necessary, instructs blocking the customer who carried out unusual activity over a certain threshold without proper explanation and/or supporting documents.

A significant vulnerability in this context derives from the concern of carrying out a series of bank transfers in amounts that do not reach the threshold set forth under the order in attempt to avoid the identification, record-keeping and reporting obligations. At the same time, it should be noted that the Postal Bank has automated monitoring and control functions, which triggers red lights or pop messages when transactions are carried out in certain amounts within a specified period of time. In light of the aforementioned, **the risk in this field is rated at a moderate - low level.**

- **Fictitious Accounts and Shell Companies**

These accounts serve as a pipeline for carrying out transactions for another beneficiary, who does not perform the transaction, and who was not recognized as beneficiary at the time the account was opened. Therefore, the threat is rated at a moderate-low level. The monitoring measure that the Postal Bank conducts include KYC process and an attempt to understand the structure of the company's holdings in the group and locating the related parties, as the Postal Bank Order and the Fit & Proper Management Instructions with respect prohibit opening an account without obtaining various documents, in addition to the standard requirements. In light of the aforementioned **the risk inherent in this field is rated at a moderate-low level.**

- **Anonymous Cards**

The threat inherent in this area derives from the purchase of anonymous cards up to 1,000 NIS per card, which may be used to pay for illegal activity. Starting from the third card, the buyer's name and ID are registered. In this context, it should be remembered that terrorist financing activity is carried out in small amounts, and therefore the monitoring measurers are significant. Therefore, the threat is rated at a moderate-low level. The vulnerability is that transfers may be made without identifying the source and destination of the funds, and below the threshold that requires KYC process. However, due to the limitation of the activity threshold per card, the vulnerabilities are rated at a moderate-low level. In light of the aforementioned **the risk inherent in this field is rated at a moderate-low level.**

## Money Service Business

Up until May 1, 2016, the supervision over MSB's was carried out by the CMISA at the Ministry of Finance. After this date, the responsibility was temporarily transferred to the Tax Authority. The Supervision of Financial Services Law (Regulated Financial Services), 5776-2016, established a new financial regulator for the regulation of the sector of Financial Services Providers, including Non-Bank Credit Service Providers and Services Providers in a financial asset. The law came into effect in June 2017 with regard to Non-Banks Credit Services Providers which are supervised by the CMISA, and in June 2018 it will take effect with regard to Service Providers in Financial Asset.

As of the beginning of 2015, the volume of the financial activity in the Money Service Business sector was estimated at approximately 120 billion NIS a year, while the number of reports received by the Israel Money Laundering and Terror Financing Prohibition Authority from this sector were not consistent with the aforementioned volume of activity, which indicates a partial understanding of the of the risks of money laundering inherent in their activity.

The vulnerabilities with respect to Money Services Business include, *inter alia*, difficulty in supervision due to the supervision unit's resources whose scope in relation the market's scope and size does not enable supervision of the entire sector; a low entry threshold to engage in the field, as well as types of financial actions that do not fall within the definitions of the Money Service Providers in accordance with the Prohibition on Money Laundering Law (such as loans and virtual currencies). At the same time, the Supervision of Financial Services Law is intended to mitigate these deficiencies and to establish significant monitoring measures, including licensing requirements, honesty and integrity examinations of the sector's operators, instructions for prohibition of money laundering and terror financing, and more.

In order to cope with the exposure to the risks of prohibition of money laundering and terror financing, the sector must implement quality controls that ensure the implementation of the prohibition money laundering and terrorism financing instructions, as well as effective measures for tracking, monitoring and managing the risks, taking into account all of the risk factors. For this purpose, the MSB Supervisory Unit reviewed, mapped and evaluated the main risk factors for money laundering and terror financing relevant to the activity of Money Service Business, as follows:

| **Customers, products, and financial services** | **Risk assessment** |
|---|---|
| **International transfers** | High (5) |
| **Accounts of corporations registered offshore** | High (5) |

| | |
|---|---|
| **Transfers to and from countries at risk** | High (5) |
| **Transfers from offshore countries** | High (5) |
| **Foreign corporations** | High (5) |
| **Foreign residents** | High (5) |
| **Foreign employees** | High (5) |
| **Foreign PEP** | High (5) |
| **Domestic PEP** | High (5) |
| **Gambling activity** | High (5) |
| **Occasional customers** | Moderate - high (4) |
| **Customers whose engagement is made through a third party** | Moderate - high (4) |
| **Customers with high-cash activity businesses (over NIS 0.5 million annually)** | Moderate - high (4) |
| **High-cash activity private customers (over NIS 250 thousand annually)** | Moderate - high (4) |
| **Customers whose origin of their capital/property is not clear** | Moderate - high (4) |
| **Use of bank checks** | Moderate - high (4) |
| **Use of virtual coins (Bitcoin and others)** | Moderate - high (4) |
| **Customers that are NPO** | Moderate - high (4) |
| **Customers who engage in the diamond sector** | Moderate - high (4) |
| **Checks discounting activity after the date of their repayment** | Moderate - high (4) |
| **Customers with a complex corporate structure** | Moderate (3) |
| **Customers executing complex transactions** | Moderate (3) |
| **Customers engaging in the precious metals sector** | Moderate (3) |
| **Israeli citizens that do not reside in Israel** | Moderate (3) |

| | |
|---|---|
| **High check depositing private customers (over NIS 250 thousand annually)** | Moderate - low (2) |
| **Use of electronic wallets** | Moderate - low (2) |
| **Currency exchange** | Moderate - low (2) |
| **Use of credit cards** | Moderate - low (2) |
| **Factoring** | Moderate - low (2) |
| **Money Service Business' customers** | Moderate - low (2) |
| **Use of travelers checks** | Low (1) |
| **Hired employees/receiving wages from known employers** | Low (1) |
| **Customers with whom the business engagement is long-term** | Low (1) |
| **Customers who engage in the pharmaceutical sector** | Low (1) |
| **Customers of services that are not face-to-face or that had been identified by alternate means** | Low (1) |
| **Customers who engage in the real-estate sector** | Low (1) |
| **Customers who engage in the import - export sector** | Low (1) |