

Israel: The Impact of the Anti-Money Laundering Legislation on the Banking System

Ruth Plato-Shinar

INTRODUCTION

In 2002 the Prohibition on Money Laundering Law, 5760–2000 entered fully into force in Israel. The object of the Law, as is evident from its name, was to combat the serious and widespread phenomenon, both in Israel as well as throughout the world, of money laundering originating in criminal activity.

The Prohibition on Money Laundering Law deals with money laundering from a number of aspects. First, money laundering is criminalised, and determined to be an independent offence. The actual act of money laundering, regardless of the original offences from which the laundered money derived, constitutes an independent offence.¹ Secondly, the Law imposes extensive obligations on financial institutions, recruiting them, against their will, to the war on money laundering. Financial institutions are required, *inter alia*, to identify their customers and to know and become familiar with their customers' activities and the nature of their businesses, a duty known throughout the world as 'know your customer'. Financial institutions are also required to report to the authorities on various transactions performed by their customers, in particular with respect to those transactions where money laundering is suspected.² A further chapter of the Law deals with obligations to report on monies entering or leaving Israel, in order to prevent the transfer of cash between states.³ Another chapter is devoted to money changers and providers of currency services who had previously not been subject to any regulatory control.⁴ One of the most significant innovations of the Law was to establish the Israel Money Laundering Prohibition Authority and set up a database on unusual transactions and activities or those where money laundering was suspected.⁵

The Money Laundering Law is broad in its scope. Its enactment was followed by extensive secondary legislation. The Law has important economic and social implications, while also raising serious ethical and philosophical questions. This paper will focus on one aspect of the Law, namely, the impact of the Law on one category of financial institutions — the banks.

BACKGROUND TO THE ENACTMENT OF THE LAW⁶

Over the last decade Israel has become a haven for money launderers. A number of factors are responsible for this, including the development of organised crime in the former Soviet Union states, with a simultaneous strengthening of economic and diplomatic ties between Israel and these states; the liberalisation of foreign currency regulations and encouragement of financial investments in Israel; stringent rules safeguarding banking secrecy, that were prevalent in Israel; a change in the economic map of the Middle East as a result of the peace process between Israel and the Arab states, and the opening of new options for bringing money into the region, as well as new drug trafficking routes.⁷ The fact that other countries took action to eliminate money laundering from within their borders meant that money launderers had to move to other countries that had not yet implemented such measures, including Israel. Israel's inactivity even caused the Financial Action Task Force (FATF)⁸ to issue a warning about money laundering in Israel. The pressure reached its height in the FATF report published in June 2000. The report included a 'blacklist' of 15 non-cooperative states in which Israel appeared alongside such states as the Dominican Republic, the Cook Islands, the Marshall Islands, the Philippines, Russia and Lebanon.⁹ The aforesaid report also determined that blacklisted states would be subject to various economic and commercial sanctions. Following this report the American Finance Department published a warning concerning transactions with Israeli entities, including the Israeli financial system. A similar warning was also published in other states.¹⁰

Actually, it had already been understood by the beginning of the 1990s, that a law needed to be enacted in Israel to combat money laundering. The legislative process for the Law took seven years, a lengthy period at anyone's reckoning, due to the protracted discussions that took place between the Bank of Israel, the Banks' Union, the Ministry of Justice, the Israel Police, various tax authorities, the General

Security Service and other entities.¹¹ The Prohibition on Money Laundering Law, 5760–2000 was eventually enacted in August 2000, but did not enter fully into force until 17th February, 2002. Around this date various secondary laws were also enacted to implement the provisions of the Law. The ‘Competent Authority to Combat Money Laundering’ was established and a database was set up for information on irregular or suspicious transactions. Israel complied with all the FATF requirements and was consequently removed from the blacklist.¹² The American Department of Finance warning was cancelled,¹³ the banks in Israel obtained the status of Qualified Intermediator, granting them concessions in the performance of transactions and trading in American securities.¹⁴

PROHIBITION ON MONEY LAUNDERING LAW, 5760–2000

The main provisions of the Law with respect to the banking system will be set forth below.

Offences under the Law¹⁵

The Prohibition on Money Laundering Law prescribes three offences. Two are called ‘money laundering’ and the third is called ‘performing a property transaction on prohibited property.’

The first offence of money laundering is prescribed in s. 3(a) of the Law, and is defined as ‘performing a property transaction on prohibited property with the object of concealing or disguising its source, the identity of its owner, its location, its movements, or the performance of a transaction with respect to such property’. ‘Prohibited property’ is defined in the section as property originating, directly or indirectly, in an offence, or used to commit an offence or enabled the commission of an offence. An ‘offence’ is one of the offences specified in the First Schedule to the Law, including trafficking in dangerous drugs, illegal trading in arms, gambling, bribery, murder, damage to property, vehicle theft, forgery of banknotes and coins, breach of copyright, terrorism, money laundering in connection with these offences, etc (but not tax offences). The legislature was not content to restrict itself to drug offences, and rightly so. By expanding the spectrum of offences it would be possible to counter additional serious crimes, such as terrorism. This is also in conformity with the international legislation¹⁶ and laws in other states.¹⁷

The terms ‘property transaction’ and ‘property’ are

also defined broadly¹⁸ to prevent any legal routes of escape. The use of this offence is directed against the money launderers themselves, and requires proof of the *mens rea* of the object of the transaction.

The second offence of money laundering is determined in s. 3(b) of the Law and deals with avoidance of reporting. The offence is ‘performing a property transaction or delivering false information with the object of preventing any reporting by providers of financial services . . . to cause incorrect reporting. The element ‘delivery of false information’ also includes failure to deliver updated information about any item required to be reported on. An example of such an offence is where a person opens an account and fails to deliver true identifying particulars, or deposits money in an account (a property transaction) and fails to provide a true report, all in order to avoid reporting with respect to such transaction. The section refers to all property and not just prohibited property, to make things easier for the police and exempt them from having to prove any connection between the property and the offence.

Both these offences of money laundering have identical penalties of 12 years’ imprisonment or a fine of NIS3m (New Israeli Shekels).¹⁹ The penalties were made severe on account of the negative consequences in the commission of such an offence and the severe breach of public order.²⁰

The third offence established in the Law is prescribed in s. 4 of the Law and is called ‘performing a transaction with prohibited property’. The offence is performing a transaction with property knowing that it is prohibited property, where the property is of the category of property specified in the Second Schedule to the Law and at the value determined therein (such as *objets d’art*, real estate, antiquities, carpets, securities, precious stones and metals, means of transportation and additional items valued at in excess of NIS120,000 or monies, bankers’ drafts, travellers’ cheques, financial deposits, investments in financial assets and other financial means valued at in excess of NIS400,000).²¹

Section 4 will apply in two kinds of circumstances. One is against the money launderers themselves, in circumstances where it is impossible to prove the *mens rea* required for the offence under s. 3(a). The second is against any person aiding a money launderer with the knowledge that he is performing a transaction with prohibited property, such as a bank, an attorney or a trader selling property to the money launderer in consideration for obtaining

'black market' money. The penalty for such an offence is seven years' imprisonment or a fine of NIS1.5m,²² a less severe penalty than that prescribed for the offences under s. 3.

The offence under s. 4, as opposed to the offences specified in s. 3, does not require an intent to conceal or disguise.²³ Instead, the section is satisfied with the knowledge that the property is prohibited property.²⁴ Under the Israeli Penal Law, 5737–1977, knowledge includes wilful blindness.²⁵ However, s. 4 of the Prohibition on Money Laundering Law specifically provided that actual knowledge that the property was prohibited was required and not just wilful blindness for this purpose. This provision is astonishing since it restricts the criminal dimension to the money launderer himself and the person with actual knowledge who helped him, whereas a person aiding a money launderer, who was wilfully blind, is exempt from criminal liability under the section. There had to have been a reason for the legislature to determine in the Penal Law that knowledge included wilful blindness and in the author's view there is no reason to determine a different rule for offences under the Prohibition on Money Laundering Law. Moreover, such a determination does not conform with the rationale of other sections of the Law and with the enactment of the secondary legislation promulgated after the Law.²⁶ It would therefore seem to be desirable to eliminate the determination according to which only actual knowledge is required.²⁷

Section 6 of the Law prescribes three limitations without which a person will not be criminally liable under s. 4. The first limitation applies to a person who reported to the police in the manner prescribed in the Regulations prior to performing the property transaction, of his intention to perform the transaction with regard thereto and who has acted in accordance with police instructions. In accordance with this provision the Prohibition on Money Laundering (Reporting to the Police) Regulations, 5761–2000 were promulgated. The second limitation applies to a person reporting to the police as aforesaid after having performed the transaction as promptly as possible in the circumstances after the transaction has been performed. The third limitation applies to providers of financial services who are required to report by virtue of s. 7 of the Law, if they did indeed report under the provisions of the Law applying to them. To prevent people being fearful of reporting, s. 25 of the Law provides that notwithstanding the

provisions of any law, the identity of any person who acts as provided in s. 6 shall not be disclosed.²⁸ It should be noted that the exemption is only valid with respect to criminal responsibility under s. 4 and not with respect to the offences in s. 3.

Section 5 of the Law provides, with respect to each of the three offences, that it will be sufficient if the person performing the transaction knew that the property was prohibited property, even if he did not know to which specific offence the property was connected. This provision is understandable with respect to the offence in s. 3(a) (performing a property transaction on prohibited property with the object of disguising information with respect thereto) and the offence in s. 4 (performing a property transaction with specific prohibited property knowing that it is prohibited property). However, it is not exactly clear how it combines with the offence in s. 3(b) (and preventing reporting) which does not relate specifically to prohibited property.

It is clear that each of the three offences is directed against professional money launderers or persons acting in collaboration with such persons. However, are banks or their employees also liable for commission of these offences? The offences in s. 3 are only pertinent in the case of banks where they intentionally aid money laundering, which is unlikely in the Israeli banking system. With respect to the offence in s. 4, criminal liability will be restricted solely to those rare cases, if any, where the bank performs a transaction with actual knowledge of the criminal source of the customer's money,²⁹ although if the bank fulfils its duty of reporting imposed on it in the Law, it will not bear any criminal liability in view of the third limitation in s. 6 of the Law.

Chapter 3 of the Law — Obligations imposed on providers of financial services

Chapter 3 of the Law deals with the obligations imposed on banks and other providers of financial services. This chapter creates a statutory framework and recruits these providers of financial services into the war on money laundering. The chapter was the result of recognition that neither the state nor the financial institutions would be able to succeed alone in combating money laundering, but that they would have to act in cooperation. This recognition was visible legally both in the international initiatives against money laundering³⁰ and in the legislation in the various states.³¹ Chapter 3 has a double objective.

First, to prevent the banks from being utilised as a tool in the hands of the money launderers. Secondly, to attach the banks to the law enforcement system by reporting and delivery of information. Section 7 authorises the Governor of the Bank of Israel to impose obligations on the banks. There are three categories of obligations:

First, the obligation of identification. Certain services may not be rendered without obtaining the identifying particulars of the person receiving the service. The section authorises the Governor of the Bank of Israel to determine by order who shall be deemed a recipient of a service; this determination may include a beneficiary of a transaction and a trustee. Beneficiary was defined in the past as a beneficiary under the Trust Law, 5739–1979, but this definition was amended and is currently: 'a person for whom or to whose benefit the property is held or a property transaction is performed, or who is able to direct a property transaction, either directly or indirectly'. The object of the amendment was to expand the scope of those persons subject to the obligation of identification and prevent any circumvention of the Law.

The second obligation is the obligation of reporting. Banks are obliged to report on certain transactions to a special database set up by virtue of the Law. A substantive determination which will be returned to in more detail below appears in s. 7(c) of the Law according to which 'categories of reporting whose disclosure or inspection is prohibited' may be determined by order. A person disclosing any matter or allowing the inspection of a report contrary to an order shall be liable to one year's imprisonment. This is a broad provision prohibiting the disclosure of both the content and the existence or non-existence of a report.³²

The third obligation is the obligation to keep and maintain records for a certain period of time.

A fourth and additional obligation is provided for in s. 8 of the Law itself. Each bank is required to appoint a person responsible for fulfilment of the obligations imposed on the bank under s. 7. The responsible person shall act to fulfil these obligations, direct and supervise the employees with respect to fulfilment thereof.

What happens should a bank fail to fulfil the obligations imposed on it under the Law? Contrary to the situation in other states,³³ non-compliance with these obligations is not in itself a criminal offence. The sole sanction against a bank in such circumstances is a

financial sanction by virtue of s. 14 of the Law.³⁴ Only where a bank intentionally prevents reporting knowing that money laundering is involved will it be liable under s. 3(b) or s. 4 of the Law, and obviously will not enjoy the benefit of the exemption determined in s. 6 of the Law.

What should the Supervisor of Banks do to ensure that the banks fulfil their obligations under Chapter 3 of the Law? The Prohibition on Money Laundering Law, as originally enacted, failed to answer this question. In April 2002 the Law was amended and a special chapter was added, as Chapter 4 (2), dealing with powers of supervision.

Section 11n of the amended Law provides that to supervise the implementation of the provisions of the Law by the banks the Supervisor of Banks must appoint inspectors.³⁵ These inspectors were granted extremely broad power. Under s. 11n(b) they may demand from any interested party to hand over to them information and documents, including computer material. They may enter any place in which the bank is operating and conduct an onsite inspection. The inspectors are also authorised to seize any document, if they have reasonable grounds to believe that the document is necessary to prevent the breach of any reporting obligations.³⁶ The above is in addition to their powers under the provisions of any other law. It should be noted that under s. 5 of the Banking Ordinance, similar powers have already been granted to the Supervisor of Banks and persons acting under his authority. Section 11n is particularly necessary for inspectors of other financial entities subject to Chapter 3 of the Law, where no other law exists granting them the powers necessary for appropriate supervision.

Section 31c of the Law provides that the Supervisor of Banks shall transfer periodic reports to the head of the competent authority on his activities with respect to implementation of the provisions of the Law, in accordance with the Rules to be determined.

The legislature, which recruited the banks against their will to the war against money laundering, took pains to ensure that the banks were given appropriate protection. Section 24 of the Law provided that failure to perform any property transaction, including one with prohibited property, disclosure or non-disclosure, reporting or any other act or omission under the provisions of the Law, made in good faith, shall not constitute a breach of the obligation of confidentiality and trust or any other obligation under the provisions of any law or

agreement, and any person who acts or fails to act as stated shall not bear criminal, civil or disciplinary liability for the act or omission. Moreover, even where a person is exempt from civil liability as aforesaid, the court may order him, if it deems just to do so in the specific circumstances, and in the manner it sees fit, to return what he received from the other party or to pay the value thereof, or to perform the counter-obligation, in whole or in part, if the other party has performed his obligation.

Section 24 grants the banks, where acting in good faith under the provisions of the Law, a total exemption from liability. The rationale for the section is clear: the banks cannot be recruited to the war against money laundering against their will and ordered to perform complicated tasks,³⁷ while at the same time being made absolutely liable for the consequences of their acts, for good or for bad. However, the consequence of the section is that if a customer incurs damage due to the bank's conduct, the customer will bear the damage and not the bank.

A further possible solution is to provide that the bank will bear liability although the state treasury will indemnify the bank, should it be obliged to pay damages to the customer.³⁸ In such a case neither the customer nor the bank will bear liability for the damage, but the state, whose interest is first and foremost to combat money laundering.³⁹ The indemnification method requires the determination of clear criteria for receiving indemnification. It seems, for example, that a customer's demand to the bank for compensation is insufficient, as such a demand may encourage customers to submit false demands, knowing that the Treasury will eventually bear liability for the damage, and even open up the way to collusion between banks and their customers. Alternatively, it may be determined that payment of indemnification will be performed after obtaining a judgment determining the liability of the bank for the customer's damage. Moreover, the indemnification method has to ensure that the banks will not be prejudiced in consequence of complying with the provisions of the Law. Therefore, it should be determined that the amount of indemnification is to include not only the amount of damages which the bank is obliged to pay the customer, but also the expenses of the bank for conducting the case against the customer, and any damage or loss incurred by it as a result of compliance with the provisions of the law. Furthermore, assurance needs to be made that the state will not delay payment of the indemnification,

thereby causing harm to the bank during the interim period.

Enforcement and sanctions

Enforcement of the Law is implemented on two levels: the criminal and the civil. On the criminal level, penalties of imprisonment and fines were determined for the offences provided in the Law.⁴⁰ On the civil level, a financial sanction was determined.⁴¹ Where a person is in breach of the provisions of s. 7 of the Law (the section imposing obligations on financial institutions), a special committee⁴² may impose on him a financial sanction. Where the person in question is employed by the financial institution, the sanction may be imposed on the institution. Furthermore, a financial sanction may also be imposed on a financial institution that has failed to appoint a person responsible for compliance with the obligations stated in s. 8(a) of the Law. The amount of the sanction is up to NIS1.5m.⁴³ In accordance with the above provision the Prohibition on Money Laundering (Financial Sanction) Regulations, 5762–2002,⁴⁴ were enacted determining, *inter alia*, the working arrangements of the committee, criteria for imposing a financial sanction, the rates of the sanction for various breaches and rules with respect to appeals against a decision of the committee to impose a sanction.

An additional sanction determined by the Law is forfeiture. Section 21 of the Law provides for criminal forfeiture: a court convicting a person for an offence under s. 3 or s. 4 of the Law is obliged, in addition to the penalty imposed, to order the forfeiture of any property whatsoever of the offender, amounting to the value of the property relating to the offence. Experience throughout the world has proved that a sanction nullifying the proceeds of money laundering is more effective than a lengthy term of imprisonment, after which the offender is free to make use of the proceeds of the money laundering remaining in his possession.⁴⁵ The court may only in exceptional circumstances, on special grounds to be recorded, not order the forfeiture.⁴⁶ Additionally, s. 22 of the Law provides for civil forfeiture. The District Court, on the application of the District Attorney, may order the forfeiture of property in civil proceedings, where it is satisfied that the property was obtained, directly or indirectly, by an offence under s. 3 or s. 4 of the Law, and on condition that the suspect is not present permanently in Israel or cannot be found and thus an indictment cannot be

submitted against him or that the aforesaid property was discovered after the conviction.

The Competent Authority and the Database

One of the most important innovations of the Law was the establishment of a database to receive reports on irregular or suspicious transactions and activities from banks and other entities under an obligation to report. Chapter 8 of the Law regulates this matter. The Justice Ministry established a database for reports received under the Law (hereinafter: the Database)⁴⁷ as well as a competent authority with respect to the Database (hereinafter: the Competent Authority).⁴⁸ The functions of the Competent Authority are to manage the Database, process the information in the Database, ensure that such information is secure, decide on the transfer of such information to the entity competent to receive the information under this Law, and to receive and transfer such information to the aforesaid entity, all for the implementation of the provisions of the Law. The authority combines the information with other sources and attempts to consolidate an intelligence picture with respect to suspected money laundering or the funding of terrorism. The authority is an intelligence entity, not an investigative entity.⁴⁹

A more sensitive issue is to whom the Competent Authority is authorised to transmit the information received, including also financial information handed over to it by the banks, and which is supposed to be protected, *prima facie*, within the scope of the rules on banking secrecy.

Under the Protection of Privacy Law, 5741–1981, the transmission of information between official entities is permitted under certain conditions. To allow for maximum protection of the information in the Database, s. 30(a) of the Prohibition on Money Laundering Law provides that notwithstanding the Protection of Privacy Law, the Competent Authority shall not transmit information from the Database except in accordance with the provisions of the Prohibition on Money Laundering Law.

Section 30 of the Prohibition on Money Laundering Law determines several entities with authority to receive information from the Competent Authority. According to s. 30(b), the Competent Authority may transmit information to the Israel Police, upon a reasoned application, for the purpose of combating money laundering.⁵⁰ Under subsection (c), the Authority may transmit information to the General

Security Service, upon its application, for the purpose of combating terrorist organisations and protecting national security. Under s. 30(f) the Authority may transmit information to a similar authority in another state, provided that the information relates to property originating in an offence as stated in s. 2 of the Law. We therefore regard the legislature as *prima facie* protecting the confidentiality of the information and the privacy of those persons about whom reports have been made in the Database. The information may be transmitted to only three entities and for well-defined objectives.⁵¹ The Explanatory Note to the Bill stated: ‘The object of the proposed clause is to provide for maximum protection of the information within the Database and of the privacy of those persons about whom the information relates, since naturally much of the information reaching the Database relates to legitimate economic activity.’⁵²

Furthermore, s. 31A was added in the amendment to the Law, headed ‘Confidentiality’ and provides that a person obtaining information under Chapter 3⁵³ or 4 (2)⁵⁴ of the Law within the scope of his employment, shall keep such information confidential and shall not make any use thereof, except under the provisions of this Law or under a court order. A person acting in contravention of the provisions of this section shall be liable to imprisonment or a fine. This will also be the law in the case of a person negligently causing the disclosure of such information to another person contrary to the provisions of this section. The legislature chose not to limit itself to the clauses on confidentiality found in the existing law⁵⁵ but created a new confidentiality clause which also incorporated an offence of criminal intent, as well as an offence of negligence.⁵⁶ The wording of the section obliges the banks to keep confidential both information on the customer (subject to obligations to disclose to the authorities under law) as well as information against the customer, such as on the existence of a report or investigation about such customer. Since the second part is regulated by s. 7(c) of the Law mentioned above, it seems that the main part of the confidentiality clause is to protect the confidentiality of the customer.

However, the legislature was not always consistent in following this line of protection of information. Under s. 30(g), the police and the General Security Service are obliged to use the information received only for three purposes: to combat money laundering, to combat terrorist organisations and the defence of state security. However, the clause continues by

determining in the same breath that they may, within the scope of their functions, make use of any such information received from the Competent Authority, in order to investigate and prevent further offences, to detect offenders and bring them to trial, 'all in accordance with rules to be prescribed'.⁵⁷ The original version of the Law expressly prohibited making use of the information for the purpose of investigating tax offences, although this prohibition was deleted in the amendment to the Law.⁵⁸ This clause is regarded as breaking through the narrow range of objects for which the Authority was authorised to transmit information. Possibly in the future use will also be made of this information for investigations into tax offences and other crimes.

Furthermore, s. 30(h) provides that: 'Notwithstanding the provisions of any law, information received under this section shall not be transmitted to another authority except for the implementation of this Law or for the objectives specified in subsection (g).' Subsection (h) is drafted in a negative manner, as if restricting the transfer of information. It was also drafted after considering the possibility of transfer of information between authorities under the Protection of Privacy Law. However, in effect it operated in completely the opposite manner. It expanded the ambit of entities entitled to receive information from the Database. The section also enabled information to be obtained indirectly from the Competent Authority from those entities having themselves obtained the information from the Competent Authority. Section 30(h) purportedly restricts the transmission of information to the purposes specified in s. 30(g), but, as mentioned above, s. 30(g) itself is not the limit as far as the possible objects for transmission of information are concerned. It is considered that in fact the range of entities entitled to receive information from the Competent Authority has also been pierced.

Under s. 30(e) the Competent Authority may, at its initiative, transmit information for the purpose of preventing offences under the Prohibition on Money Laundering Law, the defence of state security or to combat terrorist organisations, to 'any person competent to receive information under this Law'. According to the Explanatory Note to the Bill, the intention is to those cases in which the Competent Authority suspects, while processing the information in the Database, the commission of an offence of money laundering, terrorist activity or activity against state security.⁵⁹ However, as stated above, in

light of subsections (g) and (h), there is no clear demarcation of those entities entitled to receive information under the Law. The author therefore considers that banking information transmitted to the Database is also likely to be utilised by other authorities for various purposes.

A further issue relates to the flow of information in the opposite direction, *viz.*, where the Competent Authority wishes to obtain information for the purpose of performing its functions. The legislature provided the Competent Authority with several tools to obtain information from others (apart from the reporting obligations under the Law). Under s. 31(a) of the Law the Competent Authority may demand information from the tax authorities.⁶⁰ Under subsection 31(c), the Competent Authority may demand from the banks and other entities having obligations imposed on them to report to the Database, any information required to complete a report received in the Database or in connection therewith and relating to the person about whom the report was received. These are the direct sources for obtaining information. However, the authority may also extract information indirectly by virtue of s. 30 of the Law, a clause which according to its heading deals with the transmission of information from the Database and not vice versa. Under subsections 30(b)(2) and (3), where the police and the General Security Service request from the Competent Authority to obtain information from the Database they may include in the application and reasons any information held in their possession, including information from the crime register 'and the Competent Authority may inspect such information'. This terminology shows that the Authority is unable to store the information specified in the General Security Service and police applications in the Database, but may only inspect such information on an *ad hoc* basis for a specific matter. The question is whether the Authority will use this information beyond this purpose or store it in the Database and who will supervise the Authority in this regard, since no person may inspect the Database and examine whether reporting has been transmitted to the Authority about such person.⁶¹

In this context the Prohibition on Money Laundering (Rules on Management of the Database and Safeguarding the Information in the Database) Regulations, 5762–2002 were enacted, prescribing extremely detailed rules with respect to management of the Database and safeguarding the information

therein, specifically information obtained from the police or the General Security Service. The legislature chose not to limit itself to those provisions appearing in the Protection of Privacy Law with respect to securing the information in the Database,⁶² but determined more stringent and detailed rules by Regulations.

The Database under the Prohibition on Money Laundering Law is not open for public inspection. This is clear from s. 9(a) of the Freedom of Information Law, 5758–1998 prohibiting a public authority from transmitting information which should not be disclosed under the provisions of any law.⁶³ In addition, s. 20 of the Freedom of Information Law provides that the provisions of that Law shall not derogate from the validity of any legislation prohibiting or regulating in any other manner the disclosure or transmission of information in the possession of a public authority. The transparency revolution providing the basis of the Freedom of Information Law is not evident in connection with the Database under the Prohibition on Money Laundering Law.⁶⁴

Even if the Database is not open to inspection by the public in its entirety, is a person entitled to inspect information held in the Database about himself? Section 13(a) of the Protection of Privacy Law prescribes the general rule: every person is entitled to inspect any information about him kept at a database. However, within the enactment of the Prohibition on Money Laundering Law the Protection of Privacy Law was amended and s. 13(e)(6) was added providing that a person is not entitled to inspect information about him kept at a database established under the Prohibition on Money Laundering Law. If the Database had included only information on suspicious transactions the denial of the right of inspection of the Database could be understood. However, since the Database also includes reports on innocent transactions, whose only 'sin' is their being in large amounts of money or unusual in relation to the usual activity of the customer at the bank,⁶⁵ this is possibly a denial of a basic right of the individual. Furthermore, since any person may not inspect the information kept about him at the Database by virtue of the Prohibition on Money Laundering Law, he is unable to verify the correctness of the details appearing in this Database and demand the amendment thereof, should the information be incorrect, incomplete, unclear or not updated.⁶⁶ This is particularly grave in light of the fact that the legislature exempted the bank from liability, even

where the bank has reported erroneously and caused damage to the customer as a result of this.⁶⁷

It is desirable for a person to be permitted to inspect information kept about him in the Database, unless there is a reason justifying the denial of this basic right, such as the conduct of a police or General Security Service investigation against a customer suspected of money laundering or within a set period of time after having performed the reporting in order to give the authorities time to decide whether to open such an investigation. At all events the authority should be obliged to present information upon submission of an indictment against the customer.⁶⁸

PROHIBITION ON MONEY LAUNDERING ORDER, 5761–2002

As stated above, s. 7(a) of the Prohibition on Money Laundering Law authorised the Governor of the Bank of Israel to impose obligations on banks. In January 2001 the Governor of the Bank of Israel issued the Prohibition on Money Laundering (The Banking Corporations' Requirement Regarding Identification, Reporting and Record-Keeping) Order, 5761–2002.⁶⁹ The Order imposes on banks three different obligations: identification, reporting and record-keeping.

Obligation of identification under the Order

The initial basis for the war on money laundering via the banking system was recognition by those persons involved in banking activity. Thus, the first obligation imposed on the banks was 'know your customer'.

Under s. 2 of the Order, a bank will not open an account without first recording the identifying particulars in respect of each of the account holders, authorised signatories (including authorised representatives),⁷⁰ each person requesting to open an account, beneficiaries (as defined broadly in s. 7 of the Law) and in respect of a corporate account, the holders of a controlling interest.⁷¹ Even where an account already exists and the bank is requested to add another account holder, authorised signatory, beneficiary or person with a controlling interest in an account of a corporation, this should not be done without recording their identifying particulars. The Order also imposes an obligation of identification at the time of performance of certain transactions.⁷²

Section 3 of the Order determines how the bank is to authenticate the identifying particulars and according to which documents.⁷³

According to s. 4 of the Order, when opening an account, receipt of a declaration is required from the applicant wishing to open an account. He is required to declare whether he is acting for himself or as a trustee for another person. If he declares that he is acting as a trustee, the declaration shall also include identifying particulars of the beneficiary. If there is an unknown beneficiary, the applicant shall declare accordingly. Where the account holder is not opening an account, the bank shall also demand from the account holder a similar declaration prior to performance of the first transaction in the account. When opening an account for a corporation a declaration is required of the identifying particulars of the persons with a controlling interest in the corporation. In all these cases, the declaration should be made in the format in the First Schedule to the Order, including also the undertaking to notify of any change in the particulars included within the declaration.

Section 6 of the Order prescribes an obligation of 'face-to-face identification'. The bank must identify the account holder and authorised signatory face-to-face prior to the first transaction of each of them in the account. For such purposes, 'face-to-face identification' does not have to be done by the bank itself and may be done by an Israeli attorney, or diplomatic or consular representative abroad.⁷⁴

The Order purports to determine a comprehensive arrangement with respect to identification of the persons connected to an account. The problem is that there are a number of holes that are likely to be exploited by money launderers.

A noticeable shortcoming in the Order is the absence of an obligation to receive identifying particulars from guarantors. As explained above, guarantors are the entities providing the money to the account and money launderers are likely to use this route to launder their money.

Section 2(b) of the Order requires the receipt of identifying particulars from a beneficiary. A problem arises with trust transactions where the trustee does not yet know exactly who the beneficiary is. In order not to destroy such transactions, it was determined in s. 2(b) that its provisions would not apply in the case of a trust account in favour of a beneficiary where, according to the declaration of the trustee, the identity of the beneficiary was unknown at the time

of opening the account. In such circumstances, the bank would draw the attention of the trustee, in writing, 'to his obligation to provide the banking corporation with the particulars of the beneficiary as soon as these become known'. The intention is obviously to the undertaking incorporated in the aforesaid declaration signed by the applicant wishing to open an account, according to which he undertakes to notify of any change in the particulars submitted. It would have been desirable to have imposed the obligations on the trustee in a more noticeable manner than in the form appearing in the Schedule to the Order, and by imposing sanctions on a trustee in breach of his obligation,⁷⁵ to ensure enforcement of the obligation thereby obtaining the identifying particulars of the person actually behind the opening of the account.

It is interesting to note that while the term 'beneficiary' in the Order, as in the Law, received a broad definition beyond its meaning in the Trust Law, the definition of the term 'trustee' in the Order remains limited in accordance with the Trust Law. It would have been desirable to have also expanded this term in order to prevent circumvention of the provisions of the Order. It would have also been desirable to demand identifying particulars not only from the beneficiary but also from the person creating the trust, who is also likely to hide behind the screen of a trust and actually enjoy the benefit of the monies in the account.⁷⁶

A serious deficiency in the Order is the absence of any identification requirement at the time of opening a safe deposit box.⁷⁷ The Order obviously makes an assumption that banks do not provide safe deposit boxes to the general public but only to those persons opening an account with the bank, and was therefore satisfied with the requirement of identification at the time of opening the account. However, there are likely to be unusual circumstances in this regard. In light of the fact that a safe deposit box is a means of hiding black-market money, even more vigilance should be exercised in this regard.⁷⁸

Obligation of reporting under the Order

The second obligation under the Order is the obligation of reporting to the special Database set up at the Ministry of Justice.⁷⁹ This reporting is a principal means of following up on money laundering activity.

Section 8 of the Order requires reporting on certain transactions performed by the bank where they all involve large amounts of money. For example,

deposit of cash in an account or withdrawal of cash from an account in an amount of at least NIS200,000; exchange of funds in an amount of at least NIS50,000; issue of a banker's draft in an amount of at least NIS200,000; purchase of travellers' cheques in an amount of at least NIS200,000; deposit of cheques in foreign currency in an amount of at least NIS1m; transfer of funds abroad or from abroad in an amount of at least NIS1m etc.

This obligation of reporting is an objective obligation, the criteria for reporting are clear and the bank does not have to exercise any discretion on the question whether it is required to report a particular incident. This reporting may be performed by the computer system of the bank, which has been programmed accordingly.⁸⁰

A further obligation of reporting appears in s. 9(a) of the Order. The section obliges reporting on 'transactions that seem to the banking corporation to be unusual in view of the information in the possession of the banking corporation, but it need not question or clarify the facts with the service recipient'.⁸¹

It can be estimated that the intent of the section was to report on suspicious transactions. However, the section uses the term 'unusual'. In truth, the expression 'suspicious transaction' has a criminal connotation, while most of the reports coming from the banks to the Database are reports of proper transactions. Although the desire to avoid the use of this expression is understandable, this avoidance creates a lack of clarity.⁸²

What is an unusual transaction? According to the section, it will be determined in view of the information found in the bank's possession. However, the obligation of reporting is a mixed obligation, both subjective and objective, since on the one hand a decision is required which is the bank's discretion as to whether it is an irregular transaction, yet on the other hand the irregular nature is determined according to clear factual objective standards, which are the irregular nature of the transaction against the bank's past history with the recipient of the service.

Thus, even an innocent transaction, and even where the bank clerk is familiar with the circumstances and is convinced of the innocent nature of the transaction, must be reported. If, for instance, a particular customer sold shares he received as an employee at a hi-tech company and the sum of NIS100,000 was deposited by him in his account, even if the bank clerk was notified and was familiar with the circumstances of this incident and was

genuinely convinced about the deposit, he is required to report it as an unusual transaction. A further example may be seen where a customer sends his son to study abroad and requests the first time after opening the account to send money transfers abroad, even where they are not for large amounts of money, for his son's living expenses abroad. Such a transaction also requires reporting. There are many more examples. Eventually the database on reporting unusual transactions will include the majority of Israeli residents performing legal transactions via the banks.

It is difficult to believe that this was the intent of the Governor of the Bank of Israel when he drafted the Order. This obligation of reporting will impose an onerous burden on the banks. While with respect to reporting under s. 8 it is possible to adapt the bank's computer system to perform the reports automatically, the reporting obligations under s. 9 require individual personal follow-up on the part of the bank's employees and the performance of special reporting. Furthermore, such a large quantity of reports is likely to obstruct the Database to which the reports are sent.

Section 9(b) provides examples of 'unusual' transactions. For example, an activity which appears to have been performed in order to circumvent the reporting requirement applying to the bank; frequent use of a safe deposit box at the bank by a large number of people without any apparent cause; where it appears that the account holder is operating the account on behalf of someone else without having made the appropriate declaration; various transactions amounting to more than NIS200,000,⁸³ such as a transaction in an account performed by means of an authorised representative who is not registered as such with the bank; a number of withdrawal transactions immediately after deposit, without any apparent reason; transfers abroad or from abroad where the other party to the transaction is not identified by name or account number; an account transaction which is not characteristic of the account holder or of the type of account without any apparent cause; numerous deposits in an account without any apparent cause by a person who is not an account holder or authorised signatory, etc. These examples are examples of transactions which are not just 'unusual' but also arouse real suspicion. These examples create a completely subjective reporting requirement because they require the exercise of discretion on the part of the bank when determining whether they are suspicious.⁸⁴ In view of the opening part of the

section, noting that they are only examples and without prejudice to the generality of the reporting requirement on unusual transactions by virtue of s. 9(a), it seems that the Governor's intention in s. 9(a) was also towards suspicious transactions, although, as stated this was not clearly expressed in the wording of the section.

To conclude, it seems that the Order intended only two reporting obligations, an objective obligation under s. 8 and a subjective obligation under s. 9. However, according to the wording of these sections, three classes of obligation were created: an objective obligation under s. 8, a subjective obligation under s. 9(b) and an objective-subjective obligation under s. 9(a).

However it is regarded, the Israeli model is an integrated model of an objective reporting requirement with a subjective obligation. In the USA, up until a few years ago, there was only an objective reporting system with respect to any transaction over \$10,000,⁸⁵ *viz*, widespread reporting on a vast scale.⁸⁶ It was only in 1996 that a subjective reporting obligation on suspicious transactions was added.⁸⁷ On the other hand, in Great Britain⁸⁸ and in Switzerland⁸⁹ the method is based only on subjective reporting. Objective reporting is preferable from the point of view of the banks, as it is easy to implement and has less effect on bank-customer relations. Also, as far as the police are concerned, there is a disadvantage in objective reporting, since information about such a report may be leaked to the customer and endanger the investigation. On the other hand, objective reporting is widespread, imposing a heavy administrative and budgetary burden. It may also inundate the Database and make it more difficult for the Competent Authority to process the information. Objective reporting is an invasion of privacy of innocent individuals by allowing the authorities access to information about them. The greater the information available to the authorities, the more this reminds us of a 'big brother' regime.⁹⁰ It seems that a balance between the various interests and needs will be reached by integrating the objective reporting obligation — on condition that it is not too widespread — with the subjective reporting obligation.

Should the bank have a suspicion with regard to a specific transaction, is it able to report directly to the police and not to the Database? Under s. 9 of the Order, the best path is to report to the Database. Accordingly, under the third limitation in s. 6 of the Law, a bank reporting to the Database is

exempt from criminal liability under s. 4 of the Law. It is *prima facie* apparent from s. 6 of the Law that even if the bank reports to the police it can enjoy the exemption prescribed in s. 6, this time by virtue of the first two limitations prescribed therein, since not all of s. 6 is specific to banks, only the third limitation. However, even so, a bank failing to report to the Database will be subject to the financial sanction under s. 14 of the Law.

A not so straightforward question is whether a bank is required to perform any transaction whatsoever at the instruction of the customer, even if the bank suspects that money laundering is involved. There is no such prohibition in the Order. It is interesting whether it was made in this way as a negative arrangement or whether it is a lacuna. Practically speaking, it seems that the bank has to perform the requested transaction, otherwise its refusal would be likely to reveal the bank's suspicion to the customer and the possibility of the existence of a report, accordingly. It should also be noted that a suspicious transaction may afterwards turn out to be completely legitimate. The Prohibition on Money Laundering (Modes and Dates of Transmitting Reports of Banking Corporations and Entities Specified in the Third Schedule to the Law to the Database) Regulations, 5762–2002 provide that reporting on an unusual transaction shall be done as promptly as possible after performance of the transaction.⁹¹ It may thus be assumed that the bank is required to perform the suspicious transaction. On the other hand, where the transfer of funds to a foreign state is involved, and particularly to an offshore state, it would be difficult afterwards to forfeit such funds. It would have been desirable to have made express reference to this issue and determine that the bank may perform the transaction which it reported to be suspicious, unless the police, the General Security Service or the Competent Authority to combat money laundering prohibited it from doing so within a specific time, as short as possible, after the date of receipt of the report. Possibly different time periods should be determined, according to the category of transaction requested.⁹² This solution will allow the banks to perform the transaction without being required to obtain a special permit for this purpose. In this manner their day-to-day activity will not be affected and they will be less exposed to customer claims for negligent delay in performing the transaction.⁹³

The Law in its current form does not expressly authorise the police or any authority whatsoever to

instruct the bank where suspicion arises in a certain matter not to perform the requested transaction or freeze the customer's funds.⁹⁴ In the author's view it would have been desirable to vest express statutory authority in the police for this purpose.

Reporting in good faith on transactions which are suspected of being connected with money laundering but afterwards it becomes clear that they were completely legitimate may cause the customer a great deal of harm. The legislature chose to protect the bank, including its employees, in such instances. The exemption from liability provided in s. 24 of the Law protects the banks, and the customer bears the damage himself.⁹⁵

It cannot be disputed that when a bank reports to the Competent Authority under the Prohibition on Money Laundering Law about certain transactions of the customer, this involves an invasion of privacy and of the obligation of secrecy *vis-à-vis* the customer.⁹⁶ However, it should be remembered that both the right to privacy and the obligation of banking secrecy are not absolute. Reporting performed under the provisions of the law is within the bounds of a permissible invasion not imposing any criminal or civil liability on the bank.⁹⁷ For the removal of any doubt, s. 24 appears and grants banks absolute exemption from liability for any infringement of the obligation of secrecy where they acted in good faith under the provisions of the law.

A preliminary question in this context is whether the provisions enforcing the obligation to report in the Prohibition on Money Laundering Law and in the Order of the Governor of the Bank of Israel have any constitutional force in light of the Basic Law: Human Dignity and Freedom. As may be recalled, the Basic Law protects the right to privacy in s. 7 as a constitutional right. However, the Basic Law enables violation of protected rights under that Law where the conditions in s. 8 of the Basic Law have been satisfied ('the limitation clause'). In other words, the infringement must be included within the law or under the law by virtue of express authority therein, the law must reflect the values of the state, have a proper purpose and the harm caused must be proportional to the purpose ('the proportionality test'). In light of the need to eliminate money laundering, the enormous damage money laundering causes to the national and international system and the serious harm to society in general and to the financial system in particular, it seems that the

reporting requirements imposed in the Prohibition on Money Laundering Law and the Governor's Order satisfy the limitation clause.⁹⁸ The only doubt is with respect to reporting on those 'unusual' transactions where the bank clerk is aware of the circumstances of such transactions and is convinced that they are completely legitimate, although under s. 9(a) of the Order he is nevertheless required to report on them. If it becomes apparent that the object of the Order is to report on such transactions also, which as stated above is doubtful, difficulty is likely to arise in connection with the proportionality test.

Section 12 of the Order prohibits the banks from disclosing the fact of existence or non-existence of a report under s. 9 of the Order and from permitting inspection of the documents evidencing a report as aforesaid, except to the Competent Authority, the Supervisor of Banks⁹⁹ or under a court order. Section 12 is determined by virtue of express authority in s. 7(c) of the Law itself, enabling the Governor to regulate by order categories of reporting whose disclosure or inspection is prohibited, and also prescribes that any breach of the prohibition is deemed an offence in its own right. The reason for this prohibition is clear — the effectiveness of the examination and investigation. However, the damage to the customer is severe. In the context of the bank-customer relationship, this section constitutes a serious violation of the fiduciary obligation imposed on the bank *vis-à-vis* its customer.¹⁰⁰ In contrast to the obligation of banking secrecy, the fiduciary obligation is a cogent right from which the bank is unable to exempt itself.¹⁰¹ Infringement of this obligation is deemed to be a fundamental breach of contract¹⁰² and grants the customer a cause of action against the bank. Until the present no exceptions have been recognised to the fiduciary obligation, and in effect the opposite is true. The broad scope of the obligation has always been emphasised as long as the bank-customer relationship remains in existence.¹⁰³ And now the Prohibition on Money Laundering Law has come along and the legislature has granted the banks absolute exemption from liability for breach of their fiduciary obligation, so long as they acted in good faith under the provisions of the law.

Obligation to save information

The third obligation imposed by the Order on the banks is the obligation to save information. A number of sections in the Order require the banks to save various documents for a period of seven

years, so that when necessary the pertinent information from them may be extracted.¹⁰⁴ For the same reason, s. 14(a) of the Order requires banks to maintain a computerised database of account numbers and identifying particulars of the account holders, authorised signatories, beneficiaries and persons holding a controlling interest.¹⁰⁵

The obligation to save information also raises the question of the protection of customer privacy, since the majority of reports are of proper transactions of innocent customers and retaining these reports for such a long period leaves the information unnecessarily exposed.¹⁰⁶ However, we should also assume here that considerations of maintaining public order and combating money laundering will override considerations of privacy, particularly since the banks are in the practice of keeping information for a long period of time for other reasons.

GUIDELINES ON 'PREVENTION OF MONEY LAUNDERING, IDENTIFICATION OF CUSTOMERS AND RECORD-KEEPING'¹⁰⁷

As stated above, the Supervisor of Banks had already, back in 1995, issued guidelines to the banks concerning identification of customers and record-keeping. In May 2002 the Supervisor of Banks issued an amendment to the aforesaid guidelines, constituting essentially new guidelines. Even the name of the guidelines was amended to the 'Prevention of Money Laundering, Identification of Customers and Record-Keeping'.

The Supervisor's guidelines incorporated many sections. These can be divided into a number of issues, as set forth below.

Determination of internal norms on 'know-your-customer'

Section 4 of the guidelines provides that a bank's Board of Directors will determine policy on 'know-your-customer'. Under s. 8 of the guidelines the basic principles of 'know-your-customer' are policy on receiving customers, customer identification and ongoing supervision of high-risk accounts. According to s. 6, bank management will prescribe internal rules on 'know-your-customer' according to the policy determined by the Board of Directors, to assure ethical and professional standards which will prevent abuse of the bank, either intentionally or unintentionally, by criminal elements.

These sections of the guidelines complete the graduated normative system of the provisions applying to the banks, from the Prohibition on Money Laundering Law itself, as the primary legislation, through to secondary legislation in the form of the Order of the Governor of the Bank of Israel and the guidelines of the Supervisor of Banks down to the policy and internal rules of each and every bank. Such a hierarchical structure is a good base to ensure the enforcement of the law.¹⁰⁸

Identification requirement

Section 9 of the guidelines deals with customer identification and determines five rules:

A. A bank shall not open an account for a customer unless it has taken reasonable steps to determine the true identity of the account holder, the other beneficiaries of the account and the customer's authorised representatives.

B. In the event that the account holder or beneficiary of the account, is not either directly or indirectly an individual, although under the control of an individual or group of individuals, or they are the principal beneficiaries thereof, reasonable measures must be taken to determine their true identity.

C. An account may not be opened for a customer acting for a third party who fails to deliver the information required with respect to the third party in question.

D. If the bank has reason to believe that a person wishing to open an account has been refused receipt of banking services by another bank for reasons relating to money laundering, it shall operate stringent examination procedures on opening the account for the customer in question.

E. After opening an account, there should be verification of the address submitted to the bank after sending a notice to the bank according to the aforesaid address, approving the opening of the account. This obligation shall not apply if the customer requested not to send notices to the address in question.

The rules on identification determined in the section are examined below.

First, a semantic comment. The section, according to its heading and part of its subsections, deals with the identification of 'customers'. The guidelines do

not include a definition of who is a customer. In the Order enacted by the Governor of the Bank of Israel and in s. 7 of the Prohibition on Money Laundering Law by virtue of which the Order was enacted, the term 'customer' was not defined¹⁰⁹ although the terms 'service recipient', 'authorised signatory', 'account holder' etc were defined. It would have been beneficial to stick to the same terms in the legislation in order to avoid doubts on the question with respect to whom exactly the identification requirement applies.

According to the section, a bank is required to examine the true identity of the entities connected to the account by taking 'reasonable measures'. The Supervisor does not explain what these reasonable measures are, which leaves discretion with the bank clerk. Furthermore, the Order of the Governor of the Bank of Israel provides in great detail how the identification of the entities in question should be carried out¹¹⁰ so that the bank clerk is to act in accordance with the aforesaid Order and essentially the Bank of Israel guidelines in this matter become irrelevant and may even be likely to cause the failed implementation of the precise provisions of the Order.¹¹¹

An interesting question to consider is why it was determined that if a bank has reason to believe that a person wishing to open an account was unable to open an account at another bank for reasons relating to money laundering, the bank may still open an account for him. Section 2 of the Banking (Service to Customer) Law, 5741–1981 obliges the bank to provide the service of opening accounts, unless they have a reasonable ground for refusing to do so. Where a bank is aware that another bank refused to open an account for reasons relating to money laundering, this should constitute a reasonable ground for refusal to open the account for the person in question. Obviously the Supervisor of Banks did not wish to restrict the banks too much and infringe their freedom to engage in their occupation and their chance of acquiring new customers, but the question is whether this is the right case to make such a determination. At all events, if an account is opened for such a person an immediate suspicion exists against this person from the moment of opening the account. We saw that s. 9 of the Order orders the bank to report information to the Database on suspicious transactions. It appears that in the case of such a person wishing to open an account the bank will need to report both on the actual opening of the

account as well as on any transaction performed in the account.

And finally, mention should be made of the examination of the address. The Order of the Governor of the Bank of Israel demands a record to be made of the address of all the account holders, authorised signatories and any person wishing to open an account. However, despite the fact that the Order makes detailed reference to the question how to verify the various particulars submitted to the bank, there is no reference to the question as to how to verify the address.¹¹² Thus, in this regard the guidelines of the Supervisor of Banks do indeed add to the Order. However, a limitation appears in the guidelines, which is that if the customer himself requested not to be sent notices, notices should not be sent to him. There is a real reason for such a limitation. Some customers do not want their family members and others knowing of the existence of their bank accounts and fear that mail sent to them from the bank will provide evidence of this. Foreign residents in countries prohibiting the investment of funds outside these countries may fear that the authorities will discover their investment in Israel. In such instances the desire to assist such customers is understandable. However, on the other hand, professional money launderers are likely to abuse this limitation for their own purposes.

A further point on the address issue is that it would have been desirable to determine that the address must be a real address and not just a postal box, so that when necessary it would be possible to identify and even trace the customer.

On the other hand, the section dealing with the account of a corporation and requiring identification of persons behind the corporation, even if they are not directly holders of a controlling interest in the corporation, is a most important section and constitutes an important addition to the Order.

Several more sections of the Supervisor's guidelines deal with the issue of identification.

Section 10 of the guidelines requires a record of the identifying particulars of guarantors. This provision is highly important since, as stated above, the Order did not require the identification of guarantors.

Section 13 is also connected to the issue of identification. Although its heading states 'Saving of identification documents', it also deals with updating the identifying particulars in the possession of the bank. The issue of updating particulars is

highly significant. Although under the First Schedule to the Order (the declaration signed by the person wishing to open an account) the person wishing to open an account undertakes to notify on updating of particulars, this is only with respect to particulars appearing in the declaration and not with respect to all the identifying particulars submitted to the bank. Moreover, the imposition of an obligation to update on the person wishing to open an account is not sufficient and it should be expressly determined that the bank itself is under an obligation to ensure that the particulars are updated. This was done in this section of the guidelines. The section determines that the bank is required to carry out reviews to assure the existence of appropriate and updated information. Where the bank discovers that significant information with respect to a customer is missing, it must take measures to assure that the appropriate information is obtained as promptly as possible.

What happens when a person wishing to open an account or a person wishing to perform a specific transaction refuses to hand over the identifying particulars? The Order states that the bank shall not open the requested account or perform the transactions relating to which identification is required under the Order. It is particularly desirable to note s. 16(a) requiring identification in transactions 'likely to pose a significant risk to the bank'. The section does not mention the intent in connection specifically with money laundering. The wording is sufficiently broad to also include other risks and in view of the explanatory note in the preamble to the guidelines, this could possibly be the intent.¹¹³

Section 19 of the Supervisor's guidelines deals with accounts for a third party, such as accounts managed by a trustee. According to the section, a bank will take measures 'to understand the relationship' between the entities connected with such accounts. The Supervisor's guidelines are not merely satisfied with a technical identification of the person requesting the service but also demand a deeper understanding of the circumstances. Furthermore, the bank is required to record the identifying particulars of the persons setting up the trust. Hence, this is an addition to the Order, which only demands the identity of the beneficiary and the trustee.

Finally, s. 23 ensures that the bank provides its employees with appropriate training on customer identification.¹¹⁴

Suspicion and risks

Another group of sections deals with the issue of suspicion and risks.¹¹⁵

Section 14 of the guidelines obliges the banks to follow up routinely on customer account activity to decide whether it is conforming to the bank's expectations with respect to the account's activity and to trace unusual activity. Furthermore, banks need to draw up detailed internal rules regulating the manner of reporting on unusual activities under s. 9 of the Order.¹¹⁶ The internal rules should include full documentation of the decision-making process, from preliminary discovery to the formation of a decision on whether to report to the Competent Authority. Here, as with s. 9 of the Order, the wording chosen was 'unusual activity' as opposed to 'suspicious activity'.

Section 15 of the guidelines deals with accounts of customers having a 'high risk with respect to the prohibition on money laundering'. It is for the bank to define which accounts are to be considered such accounts, taking into consideration the category of business (such as businesses having high cash activity), the place of activity of the customer (such as in countries classified by the FATF as states failing to cooperate with respect to the war on money laundering, the categories of services provided by the customer (such as electronic transfers of large amounts of money), the category of customer (such as a public figure from abroad or a corporation having a complicated ownership structure). The bank is required to follow up on accounts of high-risk customers.

Section 21 of the guidelines deals with 'public figures', defined in the section as 'foreign residents holding senior public office abroad, such as mayors and heads of state, senior politicians, senior judges, senior army officers, and senior party officials, including their spouses and any corporation under their control'. The account of a customer who is a public figure is defined under the guidelines as the account of a high-risk customer and it should be managed with great caution and in accordance with the rules determined in s. 21.

Miscellaneous

Various sections of the guidelines of the Supervisor of Banks were devoted to individual treatment of specific banking services arousing particular suspicion as to their abuse by money launderers. For example, s. 12

dealing with private banking (preferential banking services given to persons owning great financial wealth); s. 18 dealing with numbered accounts (accounts where the identity of their owners is known to the banking corporation, although instead of identifying particulars, numbers or code names appear in part of the bank records); s. 22 deals with correspondent banking; and s. 27 deals with banking transfers.

CONCLUSION

In 2002, upon full entry into force of the Prohibition on Money Laundering Law, Israel joined the group of developed countries regarding laundered capital as a real risk, and aspiring to combat money laundering in any manner possible.

Experience in Israel and throughout the world has proved that money laundering is carried out in many instances by exploiting the banking system. Therefore, without obliging the banks to share the information in their possession with the enforcement institutions, and even take operative measures such as reporting on certain transactions, the state is unable to effectively combat the phenomenon of money laundering. As reviewed above, the Prohibition on Money Laundering Law, the Order prescribed by the Governor of the Bank of Israel, and the guidelines of the Supervisor of the Banks, together created an updated network of provisions, defining the war on money laundering and recruiting the banking system to the assistance of the authorities. The Law imposes a heavy burden on the banks, but without the imposition of this burden there is no chance of eradicating, or at least reducing the phenomenon of money laundering.

In the Prohibition on Money Laundering Law the state took a great step forward, although the path is still long. Without an efficient system of control and enforcement, including the imposition of pecuniary fines, and the exercise of other sanctions against those in breach of the statutory provisions, there is no chance of achieving its objectives. While agreeing with the great importance of the Law, a number of aspects and points within the Law require re-examination, both conceptually and practically, in light of the experience accumulated in its implementation.

REFERENCES

- (1) Sections 3 and 4 of the Law.
- (2) Chapter Three of the Law and the Orders issued by virtue thereof.

- (3) Chapter 4.
- (4) Chapter 4 (1).
- (5) Chapter 8.
- (6) On international initiatives to combat money laundering prior to the enactment of the Law in Israel, see Harpaz, G. and Colombo, S. (2000) 'Israel: Money Laundering at the Crossroads', *Journal of Financial Crime*, Vol. 7, No. 4, p. 351; Harpaz, G. (2001) 'Israel: Money Laundering: A Clean Break', *Journal of Money Laundering Control*, Vol. 4, No. 3, p. 264. Note further, The United Nations Convention Against Transnational Organized Crime, 40 *International Legal Materials* (2001) (hereinafter: the 'Palermo Convention'). Although this treaty was signed immediately after the enactment of the Prohibition on Money Laundering Law, the negotiations conducted prior to the signing had an impact on the Israeli legislation.
- (7) Prohibition on Money Laundering Bill, 5759–1999, Law Proposals 420, at p. 422.
- (8) An organisation set up by the heads of the G7 nations whose sole objective was to combat money laundering throughout the world. See the Internet site of this organisation, at www.oecd.org/fatf/.
- (9) www.oecd.org/fatf/NCCT.
- (10) Magen, H. (2002) 'American Finance Department Removes Warning on Transactions with Israelis Due to Suspected Money Laundering', *Globes*, 16th July.
- (11) Korin-Lieber, S. (1999) 'Blue and White Money Laundering', *Globes*, 2nd November.
- (12) Magen, H. (2002) 'Israel Removed from Blacklist of Countries Aiding Money Laundering', *Globes*, 23rd June; Zucker, D. (2002) 'Banks Breathe a Sigh of Relief', *Globes*, 23rd June; Tamkin, A. (2002) 'Just the Beginning', *Globes*, 23rd June. As of August 2002, Israel had still not been accepted as a member of FATF.
- (13) Magen, ref. 10 above.
- (14) See www.irs.ustreas.gov/business.
- (15) On the rationale for prescribing money laundering as an offence, see Allridge, P. (2001) 'Symposium: the Moral Limits of the Criminal Law: The Moral Limits of the Crime of Money Laundering', *Buffalo Criminal Law Review*, Vol. 5, p. 318 who opposes prescribing such an offence following an economic analysis of the harm caused as a result of doing so.
- (16) See the Preamble and definitions in s. 1 of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime, Europe TS No. 141, 30 *International Legal Materials* 148 (1991) (the 'Strasbourg Convention'). The definition of the term 'criminal activity' in s. 1 of the Directive of the European Union, Directive 2001/97/EC, *OJL* 344 (4/12/01) p. 76, appearing on the Internet site www.europa.eu.int and on www.oecd.org/fatf/Initiatives_en (the '2001 Directive'). Section 6(2)(b) of the Palermo Convention, ref. 6 above; Recommendation 4 of the 40 Recommendations for Measures against Money Laundering published by FATF, appearing on the website www.oecd.org/fatf/40Recs (the 'FATF Recommendations').
- (17) In the USA: 18 USC 1956 (c)(7), 18 USC 1957 (f)(2); English law: Criminal Justice Act 1993, Arts 93A–93C; Terrorism Act 2000, Art. 18; Proceeds of Crime Act 2002 (not yet in force), Arts 327–329, 340 (not yet in force as of January 2003); Swiss law: Schweizerische Strafgesetzbuch vom 21 Dez. 1937, RO 1990, 1077, Art. 305 *bis*.
- (18) In s. 1 of the Law.
- (19) As of August 2002.
- (20) Prohibition on Money Laundering Bill, ref. 7 above, at p. 423. Investigations had already commenced on suspected money laundering and bringing to trial under the new Law:

- Krau, K. (2001) 'Suspect Arrested for Laundering Millions of Dollars Stolen in Holland', *Ha'aretz*, 21st March; Zohar, A. (2002) 'Police Blitz', *Globes*, 24th June; Yarkoni, Y. (2002) 'First Time in Israel: Charges of Laundering Drug Money', *Yedioth Acharonoth*, 13th June.
- (21) According to s. 33(c) of the Law these amounts are index-linked.
- (22) As of August 2002.
- (23) Prohibition on Money Laundering Bill, ref. 7 above, at p. 423.
- (24) It is interesting to note that in the Bill's version of s. 4 express knowledge of the property being prohibited property was not required. The final version of this section in the Law is therefore different. See the debate in the Knesset on the Second and Third Readings of the Law: *Divrei Haknesset* 5760, booklet 39, 10,904.
- (25) Section 20(c)(1) of the Law.
- (26) Section 6 of the Law exempts from liability a person reporting on performing a transaction in prohibited property. Section 9 of the Prohibition on Money Laundering (The Banking Corporations' Requirement regarding Identification, Reporting and Record-Keeping) Order 5761–2001 requires banks to report on any suspicious or unusual transaction. The reporting requirement is not consistent with the allowance for wilful blindness.
- (27) To compare, in the USA the law demands knowledge, although the courts have been satisfied with wilful blindness: von Kaenel, F. J. (1993) 'Wilful Blindness: A Permissible Substitute for Actual Knowledge Under the Money Laundering Control Act?' *Washington University Law Quarterly*, Vol. 71, p. 1189; Ratliff, R. (1996) 'Third Party Money Laundering: Problems of Proof and Prosecutorial Discretion', *Stanford Law and Policy Review*, Vol. 7, p. 173 (1996); April, D. H. and Grasso, A. M. (2001) 'Money Laundering' *American Criminal Law Review*, Vol. 38, p. 1058; and in England, Howard, C. (1998) 'The *Mens Rea* Test for Money Laundering Offences', *New Law Journal*, 4th December, p. 1818.
- (28) Except in accordance with the restrictions in the section.
- (29) Harpaz, ref. 6 above, at p. 357.
- (30) The Basel Committee on Banking Regulations and Supervisory Practices within the framework of the Bank of International Settlements. The Statement on Prevention of Criminal Use of the Banking System for the Purposes of Money Laundering was published in Basel in 1988 (the '1988 Basel Rules') and Customer Due Diligence for Banks ('2001 Basel Rules') in 2001. See also, Recommendations 9–29 of FATF, ref. 16 above. Sections 3–11 of the EU Directive on Prevention of the Use of the Financial System for the Purposes of Money Laundering 91/308/EEC, *OJL* 166 (10.6.91) 77, Art. 1 ('European Directive').
- (31) In the USA: the Bank Secrecy Act (BSA), Pub.L.No. 91–508, 84 Stat. 1118 (1970), codified as USC §§1829b, 1951–1959, 31 USC §§5311–5322. This is the informal name of the Financial Recordkeeping and Currency and Foreign Transactions Reporting Act. In 1982 it was redrafted without any significant changes under the name of the Money and Finance Act. Later on several more statutes were enacted which introduced amendments to this Act: the Money Laundering Control Act of 1986, the Anti-Drug Abuse Act of 1988, the Money Laundering and Financial Crime Strategy Act of 1988, s. 2532 of the Crime Control Act of 1990, s. 206 of the Federal Deposit Insurance Corporation Improvement Act of 1991, the Annunzio Wylie Anti Money Laundering Act of 1994, the Money Laundering Suppression Act of 1992 and recently, following the attack on the World Trade Center in September 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001. English law: The Financial Services and Markets Act 2000, Art. 146 and the Money Laundering Regulations 1993, SI 1993/1933. Swiss law: Loi Federal du 10 Oct. 1997 Concernant la Lutte contre le Blanchiment d'Argent dans le Secteur Financier, RS 955.0, RO 1998 832. The French and German texts of the enactment may be found on the website www.admin.ch/ch/f/rs/c955_0.htm. An unofficial translation into English may be found at www.kpmg.ch.
- (32) In reality, the prohibition on disclosure to a customer is not new. According to the guidelines of the Supervisor of Banks on 'Proper Banking Management — Police Investigations', banks are prevented from disclosing to their customers that a police investigation is being conducted against them. The prohibition on disclosure to the customer also appears in the following sources: s. 8 of the European Directive, ref. 30 above; s. 7 of the 2001 Directive, ref. 16 above; Recommendation 17 of the FATF Recommendations, ref. 16 above; in the USA, 31 USC §5326(C); in English law, there is an offence of tip-off in Art. 53 of the Drug Trafficking Act 1994, Art. 93D of the Criminal Justice Act 1993, Art. 39 of the Terrorism Act 2000 and Art. 333 of the Proceeds of Crime Act 2002 (not yet in force).
- (33) A criminal offence provided for in English law: the Drug Trafficking Act 1994, Art. 52; the Terrorism Act 2000, Art. 21A (as amended in the Anti-Terrorism, Crime and Security Act 2001); and the Proceeds of Crime Act 2002 (not yet in force), Art. 330; in the USA, 31 USC §5322; and in Switzerland, Loi Federal du 10 Oct. 1997 Concernant la Lutte contre le Blanchiment d'Argent dans le Secteur Financier, RS 955.0, RO 1998 832.
- (34) The only exception is the above mentioned Art. 7(c) of the Law that prohibits disclosure of a report.
- (35) On those persons fit to be appointed as inspectors, see s. 11n(a)(2) and (3) of the Law.
- (36) With respect to the seizure and handling of documents, see ss 11n(b)(3) and 11o of the Law.
- (37) Such as reporting on unusual transactions. See below, in Chapter E(2).
- (38) This method was adopted in s. 14A(c) of the Checks Without Cover Law, 5741–1981. In that Law, if the name of a customer is mistakenly published as a restricted customer, the bank causing the publication shall not be exempt from liability, although the state will indemnify the bank for the amount paid in damages.
- (39) A section exempting from liability also appears in the USA. Under 31 USC §5318(g)(3), a person who reports on a suspicious transaction, either at his own initiative or upon a demand received from the authorities, shall not bear liability under the provisions of any law or agreement on account of the disclosure or on account of the fact that he failed to disclose to the person referred to in the report that a report had been made about such person. A broad exemption also appears in Swiss law: Loi Federal du 10 Oct. 1997 Concernant la Lutte contre le Blanchiment d'Argent dans le Secteur Financier, RS 955.0, RO 1998 832, Art. 11. In English law the exemption is far more limited, and protects the banks only from breach of the duty of confidentiality: the Terrorism Act 2000, Art. 21B (as amended in the Anti-Terrorism, Crime and Security Act 2001); Proceeds of Crime Act 2002 (not yet in force), Art. 330. Criticism of this may be seen in Clark, N. (1996) 'The Impact of Recent Money Laundering Legislation on Financial Intermediaries', *Dickinson Journal of International Law*, Vol. 14, p. 502. The grant of an exemption from liability also appears in Recommendation 16 of the FATF Recommendations, ref. 16 above, and in s. 9 of the European Directive, ref. 30 above.

- (40) In ss 3(a), 3(b), 4 and 7(c) of the Law.
- (41) Chapter 5 of the Law.
- (42) The committee is established by virtue of s. 13 of the Law. The section also refers to the composition of the committee and the determination of its working arrangements. Notice on establishment of the committee with respect to banking corporations was published in *Yilfut Hapirsumim* 5762, 2368. Section 17 of the Law provides a right to the person upon whom the committee intends to impose a financial sanction to present his case. Section 20 provides a right of appeal to the court against any demand for payment of a financial sanction. Section 36 of the Law provides a transitional provision.
- (43) As of August 2002.
- (44) *Kovetz Hatakanot* 248.
- (45) Maron, A. J. (1999) 'Is the Excessive Fines Clause Excessively Kind to Money Launderers, Drug Dealers and Tax Payers?', *John Marshall Law Review*, Vol. 33, p. 243; Evans, J. L. (1996) 'International Money Laundering: Enforcement Challenges and Opportunities', *Southwestern Journal of Law and Trade in the Americas*, Vol. 3, p. 197.
- (46) A court confirming the seizure of property for the purpose of its forfeiture in the future: Miscellaneous Motions (TA) reported in 'Open Account' in *Globes*, 5th August, 2002. The forfeiture clause has already been used, see Zohar, A. (2002) 'Police: Owners of Gambling Ship "Royal Casino" in Eilat Laundered Dozens of Millions of Shekels in Last Two Years', *Globes*, 4th September.
- (47) Section 28 of the Law.
- (48) Section 29 of the Law. Israel was accepted as a member of Egmont, the organisation of competent authorities to combat money laundering in various countries, currently incorporating 58 authorities. Information on Egmont may be found on the website www.ncis.gov.uk/ec.asp and on the website www.oecd.org/fatf/Initiatives_en.htm.
- (49) An interview with the head of the Israel Money Laundering Prohibition Authority, Advocate Yehuda Scheffer, appears in Dror, R. (2002) 'The Next Stage in the War Against Money Laundering Will Be the Obligation to Report of Advocates Acting as Trustees', *The Advocate*, September, p. 24.
- (50) Accordingly the Prohibition on Money Laundering (Rules on an Application for and Transfer of Information from the Competent Authority to the Israel Police) Regulations, 5762–2002 were enacted, as well as the Prohibition on Money Laundering (Rules on an Application for and Transfer of Information from the Competent Authority to the General Security Services) Regulations, 5762–2002.
- (51) This was stated in the Explanatory Note to the Bill, ref. 7 above, p. 430 and is also apparent from s. 31B(3) which was added to the Law in its amendment: Prohibition on Money Laundering (Amendment) Law, 5762–2002.
- (52) Prohibition on Money Laundering Bill, ref. 7 above, p. 429.
- (53) The Chapter dealing with the obligations imposed on financial entities.
- (54) The Chapter dealing with supervision of financial entities.
- (55) Section 117 of the Penal Law, 5737–1977. For criticism of s. 117, see Segal, Z. (2000) *The Right to Know in Light of the Freedom of Information Law*, Israel, p.190 and the references therein: s. 16 of the Protection of Privacy Law, 5741–1981; s. 65 of the Bank of Israel Law, 5714–1954; s. 15(a) of the Banking Ordinance; and s. 496 of the Penal Law, 5737–1977.
- (56) Minutes no. 453 of the meeting of the Constitution, Law and Justice Committee (25th March, 2002), at p. 13.
- (57) Under subsection (i) the Minister of Justice is competent to prescribe the additional offences referred to in subsection (g).
- (58) See the debate on the Second and Third Hearings in the Knesset on the amendment to the Law: Prohibition on Money Laundering (Amendment) Bill, 5762–2002, *Divrei Haknesset*, 30th April, 2002. The head of the Competent Authority, Advocate Y. Scheffer, confirmed this. See Tamkin, A. (2002) 'On Route to a White Future', *Globes*, 24th June, 2002.
- (59) Prohibition on Money Laundering Bill, ref. 7 above, at pp. 430–431.
- (60) Subject to the approval of the Minister of Finance. However, under subsection (b), special rules may be enacted for speedy handling of applications of the authority to obtain information.
- (61) See below the text alongside ref. 65.
- (62) Sections 17, 17A, 17B of the Protection of Privacy Law, 5741–1981.
- (63) The law in the present case is, as stated, s. 30 of the Prohibition on Money Laundering Law.
- (64) For criticism on the violation of the right to receive information from public authorities see Segal, ref. 55 above, p. 238.
- (65) By virtue of ss 8 and 9(a) of the Order. See below in Chapter 5 (2).
- (66) Compare with s. 14 of the Protection of Privacy Law with respect to information in databases, s. 16 of the Freedom of Information Law, 5758–1998 with respect to information kept by public authorities, which all grant a right to demand the amendment of the information.
- (67) Section 24 of the Order. See below in Chapter 5 (2).
- (68) Britzman, G. (2001) 'Banking Secrecy — the First Victim in the War Against Money Laundering', *Globes*, 1st February.
- (69) The Order entered into force on 17th February, 2002. Section 17 prescribed transitional provisions with respect to existing accounts.
- (70) 'Authorised signatory — someone empowered by the account holder to operate the account, whether or not the account holder is an individual, provided that he is registered in the banking corporation as someone permitted to operate the account.' This definition is different from the definition in the Checks without Cover Law, 5741–1981, which in s. 1 differentiates between an authorised representative and an authorised signatory.
- (71) The Order specifies in s. 2 which exact documents are required. With respect to a beneficiary (s. 2(b)) and a person with a controlling interest in a corporation (s. 2(c)) less identifying particulars are required, since they are more distant factors, both physically, since they generally do not come to the branch, and substantively, since they do not receive a service from the bank and a demand to receive varied particulars about them is likely to delay the opening of the account and performance of the requested transactions. The author takes the view that this should be reconsidered.
- (72) Sections 2(f) and 2(g) of the Order.
- (73) It is interesting to note that with respect to an identity certificate and foreign passport, as opposed to a registration certificate of a corporation, the section does not demand a certified copy but is satisfied with a photocopy. At the time of opening an account for a corporation, the section allows for the provisions of an attorney's certificate instead of receipt of a resolution of the competent organ in the corporation. In the author's view, it would have been desirable to have demanded an attorney's certificate in addition and not as a substitute.
- (74) In only one case is the bank required to perform the face-to-face identification itself, and that is in the event of a transaction requiring reporting under the provisions of s. 8 of the Order and is not recorded in any account whatsoever of the customer. This obligation of 'face-to-face identification' appears in s. 3(11) of the 2001 Directive, ref. 16 above. The

- Basel Rules 2001, ref. 30 above, also refer to this at length in ss 45–48.
- (75) Section 3(b) of the Prohibition on Money Laundering Law prescribes an offence, *inter alia*, of failure to update particulars requiring reporting. However, a condition for the offence is the object of avoiding reporting or causing incorrect reporting. A trustee who fails to have such an intent will not fall within the bounds of the clause.
- (76) On the creator of a trust, see Kerem, S. (1995) *The Trust Law, 5729–1969*, 3rd edn, HSL, Tel Aviv, p. 90.
- (77) Although s. 9(b)(2) of the Order requires that the bank report on any frequent use of a safe deposit box by a large number of persons without any reasonable cause, this is insufficient.
- (78) In the past a proposal was raised by the Ministry of Finance to oblige the public to report on the contents of safe deposit boxes held at banks within the framework of the fight against black-market capital. See in this regard, Plato-Shinar, R. (2000) 'The Finance Ministry Plans to Go Into the Safes Again?' *Globes*, 21st May, at p. 88. The obligation of identification relating to safe deposit boxes appears in the Basel Rules 1988, ref. 30 above, and in Recommendation 10 of the FATF Recommendations, ref. 16 above.
- (79) Section 11 of the Order provides which exact particulars should be included in the report. Sections 10 and 15(b) of the Order exempt from the obligation of reporting in certain circumstances.
- (80) This was indeed determined in Regulation 3(1) of the Prohibition on Money Laundering (Modes and Dates of Transmission of Reports of Banking Corporations and the Entities Specified in the Third Schedule to the Law to the Data Bank) Regulations, 5762–2002.
- (81) The final part of the subsection is unsuccessfully drafted. It seems that the intent was that the bank does not have to clarify the circumstances with the customer, although on the other hand the section does not prohibit him from doing so.
- (82) Use of the term 'unusual transaction' also appears in the Prohibition on Money Laundering (Modes and Dates of Transmission of Reports of Banking Corporations and the Entities Specified in the Third Schedule to the Law, to the Database) Regulations, ref. 80 above, determining the mode and times of transmission of reporting. The Regulations determine various rules for reporting a 'usual transaction' and an 'unusual transaction' within their meaning in the Order. In the international legislation and in other systems of law, use of the word 'suspicious' is more common: s. 6 of the European Directive, ref. 30 above, as well as s. 6 of the 2001 Directive, ref. 16 above, require reporting on 'a fact likely to serve as an indication of money laundering'. In Appendix 1 of the Basel Rules 2001, ref. 30 above, there is reference to 'suspicious transactions', while Rule 53 requires follow up on an account to reveal 'irregular or suspicious transactions', although Rule 55 refers to reporting on suspicious transactions. Recommendation 14 of the FATF Recommendations, ref. 16 above, refers to 'unusual transactions', although Recommendation 15 requires reporting on a 'suspicion'. Recommendation 4 of the 8 FATF Recommendations on funding of terrorism also refers to a 'suspicion'. See, www.oecd.org/fatf/TerFinance. Also, s. 7 of the Palermo Convention, ref. 6 above. In the USA, s. 31 USC §3518(g) requires reporting of suspicious transactions. Accordingly, the report form is entitled 'Suspicious Activity Report'. In English law, an offence of failure to report on a suspicion of money laundering was prescribed: see ref. 33 above. A similar terminology appears in Regulation 14 of the Money Laundering Regulations 1993. In Switzerland, Loi Federal du 10 Oct. 1997 Concernant la Lutte contre le Blanchiment d'Argent dans le Secteur Financier, RS 955.0, RO 1998 832 requires in s. 9 reporting on a suspicion.
- (83) It appears *prima facie* from this wording that if the aforesaid transactions are involved but they total less than NIS200,000, there is no reporting requirement, even if they arouse suspicion. It is doubtful whether this was the intention of the legislature.
- (84) To differentiate between subjective reporting requirements and objective reporting requirements, see Hall, M. R. (1995–96) 'An Emerging Duty to Report Criminal Conduct: Banks, Money Laundering and the Suspicious Activity Report', *Kentucky Law Journal*, Vol. 84, p. 651.
- (85) 31 USC §5325 and Regulation 31 CFR §103.29, except for certain exemptions.
- (86) For criticism of the widespread reporting obligation, see Sultzter, S. (1995) 'Money Laundering: The Scope of the Problem and Attempts to Combat It', *Tennessee Law Review*, Vol. 63, p. 143, at pp. 220–223. Attempts at attacking the widespread reporting requirement by claiming illegality and an invasion of privacy were dismissed by the courts, see Hall, ref. 84 above.
- (87) Section 31 USC §5318(g) was enacted in 1992 and the regulations implementing the Act entered into force only in 1996; Hall, *ibid.*, at p. 653.
- (88) See ref. 33 above; see also Regulation 14 of the Money Laundering Regulations 1993.
- (89) Art. 9 of the Loi Federal du 10 Oct. 1997 Concernant la Lutte contre le Blanchiment d'Argent dans le Secteur Financier, RS 955.0, RO 19998 832.
- (90) Hall, ref. 84 above, p. 679 does not decide between the two approaches.
- (91) Regulation 4(a)(2).
- (92) It is desirable to note that in s. 7 of the European Directive, ref. 30 above, express reference is made to such a situation. It states that the bank should avoid performing the transaction and notify the competent authority thereof, which has authority to order the bank not to perform the transaction. However, if failure to perform the transaction 'is likely to thwart the efforts to reveal the person actually behind the transaction' the transaction should be performed and the competent authority should be notified immediately after the performance thereof. In Switzerland the law requires that the activity be frozen with a report on the suspicious transaction: Loi Federal du 10 Oct. 1997 Concernant la Lutte contre le Blanchiment d'Argent dans le Secteur Financier, RS 955.0, RO 1998 832, Art. 10.
- (93) At all events, the banks are exempt from liability in such instances in view of s. 24 of the Law.
- (94) Section 6 of the Law grants an exemption from criminal liability to any person reporting to the police prior to performance of the suspicious transaction 'and [who] acted according to its guidelines'. However, the section does not note what happens in the case of reporting to the database and not to the police, as the banks are ordered to do. And for the most part the section relates to the issue only as a condition for obtaining an exemption from criminal liability and does not grant the police express authority in this regard. This is apparently why it adopts the term 'guidelines', as opposed to binding instructions. In *Miscellaneous Criminal Motions 5015/99 The Federation of Independent Lawyers v State of Israel*, 65(I) P.D. 657 it was held, not specifically in the context of money laundering, that the police has authority to freeze bank accounts by virtue of s. 34 of the Criminal Procedure (Detention and Search) Ordinance, which authorises the police to seize assets.
- (95) See above, at the text alongside ref. 37.
- (96) On the tension between the interest of privacy and the need

- for enforcement of the law, see Preiss, R. T. (1996) 'Privacy of Financial Information and Civil Rights Issues: The Implications for Investigating and Prosecuting International Economic Crime', *Money Laundering Control*, Dublin p. 343.
- (97) Section 18(2) of the Protection of Privacy Law, 5741-1981; Civil Appeal 1917/92 *Skoler v Jarabi* 47(v) PD 764, at 771. For criticism of the broad exceptions to the right to privacy, see Plato-Shinar, R. (2001) 'The Bank Safe Deposit Box in the Mirror of the Right to Privacy', *Kiryat Hamishpat*, Vol. 1, p. 296.
- (98) An American article explains the importance of the right to privacy, particularly with respect to financial information, but eventually reaches the conclusion that American law creates a desirable balance between the right to privacy and the anti-money laundering measures, see Pasley, R. S. (2002) 'Privacy Rights v. Anti Money Laundering Enforcement', *North Carolina Banking Institute*, Vol. 6, p. 147.
- (99) He is charged under s. 12 of the Law and referred to in s. 11c of the Law.
- (100) On the fiduciary obligation of a bank to its customer, see Ben-Ulliel, R. (1996) *Banking Law — General Part*, p. 99.
- (101) Ben Ulliel, *ibid.*, p. 106, although later on he limits this finding.
- (102) Ben Ulliel, *ibid.*, n. 144.
- (103) Ben Ulliel, *ibid.*, at pp. 102-103.
- (104) Sections 7, 13, 14(b) of the Order.
- (105) Section 14(a) of the Order. Once more, there is no reference to guarantors.
- (106) Pasley, ref. 98 above, p. 196 criticises the obligation to safeguard all documents of every customer when it is clear that not everyone is connected with crime. He believes that this is an invasion of privacy and freedom from unreasonable searches.
- (107) The Supervisor of Banks: Proper Banking Management (5/02), circular no. H-2076-06. According to s. 18 of the guidelines, several sections of the guidelines have delayed validity.
- (108) With regard to 'know your customer', see also ss 5, 7 and 8.
- (109) Except in s. 2(g) of the guidelines, and this is also apparently mistakenly, on account of the absence of any definition of this term.
- (110) In ss 3 and 4 of the Order.
- (111) Also the determination that an account may not be opened for a third party if all the details about the third party are not received is irrelevant since it is provided for in the Order itself.
- (112) Except with regard to a corporation which is not registered in Israel — s. 3(a)(4) of the Order, and with respect to a 'recognised entity' — s. 3(a)(6) of the Order.
- (113) Compare with the different wording in s. 15 of the guidelines, which refers to 'a risk with regard to money laundering'.
- (114) With regard to identification, see also ss 11, 17, 19 and 26 of the guidelines.
- (115) In addition to s. 16(a) of the guidelines.
- (116) See also s. 25 of the guidelines requiring reporting also to the Supervisor of Banks in the same exceptional circumstances.

Ruth Plato-Shinar, PhD, Lecturer, Netanya Academic College and Bar-Ilan University, Israel. The author wishes to thank Mrs O. Vago, assistant legal counsellor, Bank of Israel, for her assistance and advice.