Gross Orad Schlimoff & Co.

LEGAL REVIEW Winter 2016

Contents

The "Bold Director" - The Tzmiha Case - New important decision regarding the BJR under Israel Law 1-2

New Supreme Court's Ruling C.A. 5635/13 Koral Tel Ltd. vs. Raz et al 3

Developments in Cyber Risks in Israel
Financial Institution - Cyber Risk Management 3-4

The "Bold Director" - The Tzmiha Case - New important decision regarding the BJR under Israel Law

On June 2nd 2016, an important ruling was handed down by the Financial Court in the framework of a Derivative Action application. The court discussed the scope of directors' liability and the Business Judgement Rule. This judgement also deals with proper corporate governance to which public companies are bound in Israel and the liability of directors in this respect. The court also discussed the reliance of the Board of Directors on external legal opinions.

Background:

The subject matter of the decision is a loss sustained by Tzmiha Investment House Ltd. (hereinafter: **"the Company"**), as a result of investment in the sum of NIS 20 million in Shemen Oil and Gas Resources Ltd.

The Applicant, a shareholder in the parent company argued that the Company and its D&Os must compensate the Company for the loss it sustained as a result of this transaction. The Applicant alleged that directors and officers, who approved the transaction acted negligently, and that some of them also acted in conflict of interests.

It was alleged that the directors and officers breached, *inter alia*, their duties of trust and care, the duty to act in good faith, as well as their reporting duties.

Application of the Business Judgement Rule:

According to the Business judgment Rule, the court should not interfere with the business discretion of the company's directors, who executed their duties in good faith. The Applicant claimed that the Business Judgment Rule should not apply in this case, since the directors and officers approved the transaction in an uninformed and negligent manner. According to the Applicant, the Board of Directors did not exercise any discretion when approving the transaction and the process was tainted, since not all of the relevant data was gathered and the profitability of the transaction was not discussed. Allegedly, none of the directors demanded that the Company carry out independent examinations in respect of the transaction.

The court determined that in order to examine whether the Business Judgment Rule applies, it is necessary to examine whether the decision of the BOD was made in good faith, without conflict of interests and in an informed process. The court found that the D&Os neither acted in conflict of interests nor in bad faith a proper and "informed process". The burden to prove that the BJR should not apply lies upon the one arguing it, who must prove that when making the decision, the directors did not act in good faith, or that they were in a situation of conflict of interests or did not make an informed decision.

"An informed process" includes gathering, perusing, discussing and examining data, documents and relevant considerations. This conclusion is compatible with the provisions of Section 253 of the Companies Law, which requires a director or officer to take "reasonable means to receive information, which pertains to the business profitability of an action which is brought for his approval or of an action which is performed by virtue of his position and to receive any other information which is of importance to the matter of such actions".

In this case, the Applicant failed to prove that the process of making the decision by the Board of Directors was such that the Business Judgment Rule should not apply to it.

In this context, the court determined that:

A. **A Board of Directors is not responsible to examine the terms and details of an agreement, which it approves**. They should only understand the structure of the transaction and its commercial terms and they must ascertain that the company received quality legal advice regarding the legal issues, which must be taken into account.. Any other conclusion shall impose on the company's Board of Directors undesirable liability namely, liability for the legal quality of the agreement and for legal "mishaps" and defects in the wording of the agreement.

B. Imposing liability on the Board of Directors to examine each of the terms of the agreement, is inefficient and is incompatible with the provisions of the Companies Law regarding the authority of the Board of Directors. Section 92 of the Companies Law determines that the role of the Board of Directors is to determine the company's policy and to supervise the performance of the General Manager and his actions as well as certain additional positions stated therein. In other words, **the Board of Directors is not responsible for the actual execution of the policy determined by it.**

C. **Reliance of the directors upon legal advice** in order to make decisions is reasonable and legitimate.

D. When examining whether the directors held a sufficient discussion on the merits of the business decision, the court will examine various indications, such as the length of time during which the meeting was held, the urgency in which it was convened, the background material which was presented to the directors and other matters, to indicate the seriousness of the discussion held by the Board of Directors. However, these characteristics are not exhaustive. The case may be that there are circumstances in which an urgent meeting is justified (for example due to a tight schedule for approval of the transaction). The court shall examine the decision taking process, *inter alia* based on the minutes of the meeting and the testimonies, and will determine according to the evidence whether the directors were in fact sufficiently informed of the transaction, whether they were familiar with the background material and whether they held a sufficient discussion.

E. The court determines that **the Business Judgment Rule is intended – *inter alia*, to enable the directors of the company to make decisions, from time to time, which are "daring", decisions in which a certain risk is involved,** whilst the directors know that even if these decisions will turn out to be wrong in retrospect, the court shall not impose liability on the directors for them.

F. In order to examine the application of the Business Judgment Rule, there is also relevance to the issue of the **experience and professionalism of the directors** – when professional and experienced directors held an appropriate examination process before making the decision, the presumption that the court must honor their decision is a reasonable presumption, which gives weight to the advantage which the directors have over the court, when making a business decision.

In summary, once it is determined that the Business Judgment Rule applies, the court refrains from interfering with the decision of the Board of Directors.

Reliance on an External Legal Opinion

The court ruled that where complex issues arise, reliance on a professional consultant, who is experienced in the relevant field, may be legitimate and even desirable.

The court also determined that directors cannot and should not be experts in all fields. When they are required to make a decision, which is not in their field of expertise, the proper way for them to act is by consulting an experienced and unbiased consultant in the relevant field. Once the advice of a consultant is received, the directors are entitled (and perhaps even obligated) to rely upon it.

The court emphasized that the **circumstances of the engagement of** the lawyer should be examined, such as– who approached the lawyer? Was he approached by directors on behalf of the controlling shareholder (in case the subject matter are issues concerning the controlling shareholder's interests) or by independent directors? Whether previous approaches were made to other experts, which were rejected by the directors due to their opinion? Whether the lawyer providing the opinion does not have any interest in the issues under discussion? It is also appropriate to examine the question whether the expert himself may be **liable** towards any third party prejudiced by his opinion? The burden to prove reliance on an expert opinion shall be higher for directors acting on behalf of the controlling shareholder in comparison to independent directors.

In view of the above, the court rejected the motion to approve the claim as a derivative action.

An appeal was filed in respect of this decision.

New Supreme Court's Ruling C.A. 13/5635 Koral Tel Ltd. vs. Raz et al

New decision which regulates the time for submission of third party notices in class actions.

Recently, the Supreme Court established a new precedent with regard to submission of third party notices in class actions.

The Supreme Court ruled that if a defendant has any cause of action to claim contribution from any third party, all third party notices must be filed already at the stage of the class action application and not after the class action is approved (as was the common practice until then).

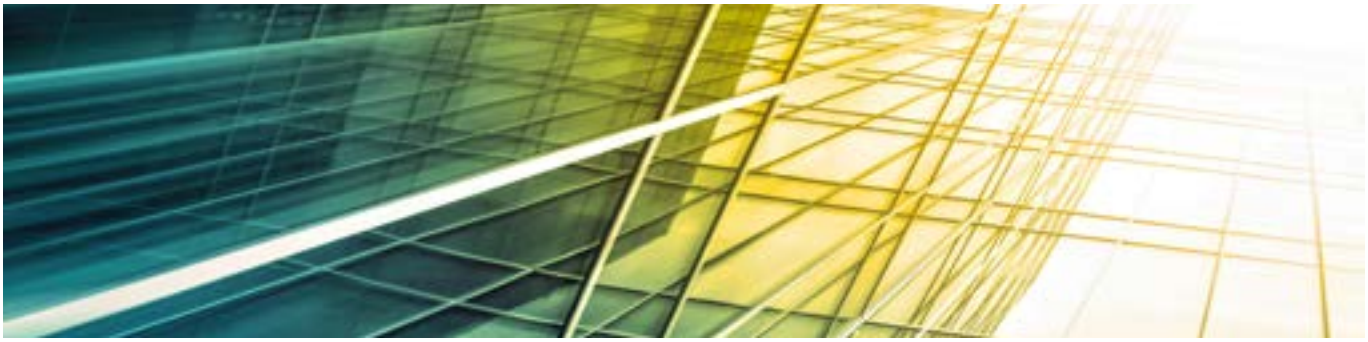
Until this ruling, usually, it was our recommendation to file a third party notice following certification of the class action application, for many reasons such as: saving costs which may be involved in filing a third party notice at this early stage, refraining from opening a front with others, which often assists plaintiff in his claim, and to receive the assistance of such third parties in the defence of the class action application.

Unfortunately, the Supreme Court did not refer in its decision to court charges. In Israel, class action plaintiffs are not required to pay court charges and as a result some of the class actions are filed at very high amounts.

The question which now arises is whether the respondents in a class action application must pay court charges with regard third party notice.

In view of the recent decision, this issue and all other considerations must be dealt with already at the preliminary stages of the class action application.

In spite of this ruling, we recommend to our clients to consider in each case whether the best solution is indeed to file a third party notice against third parties or whether there are other good alternatives which should be considered. An example of an alternative that should be considered in some of the cases is reaching an arrangement with the third parties to postpone the dispute and decide upon a certain time frame and method for resolving such dispute, for example in the framework of a separate claim or arbitration, and in the meantime to cooperate for the purpose of defending the class action application.



Developments in Cyber Risks in Israel Financial Institution - Cyber Risk Management

In view of technological developments and the increasing dependence of the Financial Institution (**FI**) on the internet network, the extent and volume of the cyber threats, which may disrupt FI's activity have gradually increased.

So far, the focus was on securing the data held at the FI computer systems. However, this is only one layer in the field of cyber risk management. Now FIs need to protect themselves from disruption of their computer systems on which their business activity is based.

Recently the Commissioner of the Capital Market and Insurance (**the Commissioner**) issued a circular in which she establishes the main principles of Cyber Risk Management of FI's and the duties of the FIs to manage such cyber risks.

The circular deals, inter alia, with the corporate governance of the FI in respect of cyber risk management. The circular refers to the duties of the FI's Board of Directors and of the CEO and states that the Board of Directors will have to approve the cyber risks management policy once a year. The Board of Directors should also appoint a Special Steering Committee to manage cyber risks.

As to the CEO, the circular states that the CEO will provide financial resources in order to implicate the cyber risks management policy and will establish the methods of reporting to the CEO, as well as other relevant factors, in case of a cyber-attack.

According to the circular, the members of the Steering Committee will be the CEO (who will act as the chairman of the Steering Committee), the Risk Manager, the Chief Information Officer and the Manager of cyber protection. The main duty of the Steering Committee is to assist the CEO in all the relevant issues relating to the cyber risk management.

The circular also establishes the framework of the cyber risk management and provides that it will include general policy, procedures, work program, and cyber protection methods, strategies etc.

The circular includes a reporting duty upon the FI to the Commissioner and the BOD, as soon as possible, regarding any significant cyber-attack which as a result its systems, which contain sensitive information, were disrupted for more than three hours or that there is an indication that information of clients, members or employees was leaked.

It should be noted that the above is only circular and no binding regulation has yet been published.

Other Developments in Cyber Risks - A First Legislative Step in the Fight Against Cyber - New Data Security Regulations

This article was written by: Adv. Dan Hay- the head of Dan Hay & Co. Legal Firm, which specializes in privacy, databases and cyber law. Our firm cooperates with him on many cyber cases.

The Israel Law, Information and Technology Authority within the Ministry of Justice (ILITA), trusted with implementing and enforcing the privacy protection laws and the security of personal information in Israel, formulated new data security regulations, which are supposed to be debated and approved in the upcoming winter-seat of the Knesset, based on an agreement between ILITA and the Counseling and Legislation department in the Ministry of Justice.

Said regulations' elaborated draft was published by ILITA in February 2010. Since then, ILITA has presented the draft in various professional conferences and seminars. After receiving extra input and commentary from the public, from agents in the business and from professional circles, and, after implementing the lessons learned from data security events associated with the notorious "Saudi Hacker" security breach in 2012, ILITA published a second, updated draft, in June 2012.

Approval of these regulations will mark a first and important step by ILITA on the subject of regulating the obligations of organizations in Israel that manage or retain personal data, and in the fight against possible cyberattacks against various organizations, private and public alike, while maintaining the principal goal of reducing the threat of the misuse of data stored by these organizations, thus minimizing the threat of a data security breach and maximizing data protection abilities.

The new regulations strive to remove the vagueness regarding data security in the current laws and regulations, which are simply not compatible with current technological status and advancements. The primary renovation that signifies the highlight of the regulations is the obligation to report to ILITA of any serious cyber-attack event amongst the various organizations that might have been exposed to a breach or exposure of their database containing personal data. Furthermore, the regulations determine the authority of ILITA in that it compels a database owner to notify the data objects regarding the breach event that occurred. On top of that, the new regulations aspire to predetermine and prepare inner-organizational procedures that will detail the procedures and capabilities of the organization in dealing with various data security events. It will also clarify the organizations' duties and the responsibilities of the various authorized personnel in the organization that have access to the data. On one hand, the purpose of the regulations is to protect the organization itself from possible harm to the privacy of the data objects and to avoid any ramifications due to failure of adhering to the legal obligations in both the criminal, civil and administrative aspects; and also, to create a uniform market, based on the customary data protection standards in the world, especially with the stringent European data protection principles, in a way that will help all parties in cooperation and dealing with mutual outer security threats like the aforementioned case of the "Saudi hacker", that could arise in the future.

The regulations' draft states a long list of actions that an organization must take in order to regularize the matter of data security within itself, while determining the duty of implanting the organization's head of data security as a direct subordinate of a senior official of the organization; as well as imposing the responsibility of implementing the aforementioned actions on the database owner. Amongst other things, each database will be required to have a "Database Definitions", or an internal road-map document that will contain a general description of the types of data within it, the data collection activity it acquires, the types of usage of the data, any transfer of the data out of the country's limits, etc.; creating a data security procedure in the organization while still giving points and detailed instruction regarding the formulation of said procedure; mapping and conducting risk surveys and defining their frequency; establishing procedures regarding compartmentalization and monitoring the usage of the data systems and the access to the databases; determining physical and environmental security procedures, in accordance with the nature of the databases activity and the sensitivity of the data within it; administering data security protocols regarding human resource management in the organization, management of access permissions and authorizations, identification and verification procedures, protocol regarding the request and issue of access permissions, etc.; documentation of security events; establishing a protocol regarding the usage of mobile and external devices in relation to the database and it's systems; secured management of the database's systems, management of connectivity and it's security, establishing backup, recovery and restoration protocols, periodic inspections, application of the responsibility of the database owner on the database manager, and more.

Finally, the draft imposes on a duty on the database owner to annually reevaluate the organization's protocols and procedures and to update them if necessary or if any of the following incidents might have occurred: substantial alteration to the database's systems or to the process of data processing; new technological threats that might be relevant to the database's systems; as a result of a periodic inspection or any other security event.

While the welcomed and necessary changes have not yet been officially approved by the Israeli legislator, they reflect the current position of ILITA, based in the existing laws and regulations, in the effort to enforce the legal directives within the organizations and bodies that manage Israelis databases.

For additional information you may contact:
Adv. Omer Shalev omer@goslaw.co.il
Adv. Laurie Shachar Laurie@goslaw.co.il

Gross Orad Schlimoff & Co.

7 Menachem Begin Rd.
Ramat-Gan 52521, Israel
Tel: 972-3-6122233
Fax: 972-3-6123322
Web Site: www.goslaw.co.il