Bank of Israel
Supervisor of Banks

July 28, 2010

Ref: 10LM0752
M10101P

To: The banking corporations and credit card companies

For the attention of the CEO

Re: Social media

1. Introduction

In the last few years the use of electronic social media such as Facebook, Twitter, MySpace, LinkedIn, YouTube, blogs and forums has surged. These networks provide a readily available means of communication and a convenient and simple infrastructure for the dissemination of information between individuals, common-interest groups, and even commercial companies. Social media can be used by banking corporations and their customers for a number of purposes—transmitting marketing material, interactive communication for handling complaints and enquiries from the public, providing general information, a channel for performing transactions in a customer's account, gathering information, etc.

2. Potential risks

Alongside the benefits that social media offer, their use also exposes banking corporations and their customers to potential risks, including operational, legal, regulatory, and reputational risks. These are likely to arise from various sources, such as:

2.1 **Customer identification**—Recording customers' particulars could expose the customer and the banking corporation to instances of social engineering and theft of a customer's identity, and damage the banking corporation's identification system. An example might be a situation in which the banking corporation relies on a customer's particulars to activate a blocked password.

2.2 **Publication of information**—The simplicity of publishing and widely disseminating information by means of the media could increase the spread of misleading, hostile, false or incorrect information by a member of staff, customer, or someone not connected with the banking corporation who wants to impair its activity. Furthermore, in light of the ease of doing so, an

employee of a banking corporation may publish information that has not been checked or approved by the appropriate parties, and without the proper control procedures being activated.

2.3 **Information security**—The websites and tools related to the social media were not necessarily created with information security among the main considerations. Their use may expose the banking corporation, its staff and its customers to such risks as viruses, Trojan horses, impersonations, and computer break-ins (hacking).

2.4 **Control**—Most of the tools used by the social media are not operated from within the banking corporation's premises and are not under its control. Hence there is no certainty that the risks were assessed and proper controls created to deal with them.

3. Risk management

In addition to Directive 357 of the Proper Conduct of Banking Business on managing information technology (IT), banking corporations must act to reduce the risks involved in using the social media, among other things by the following measures:

3.1 Assessing the risks arising from the use of the social media by them, their staff, and their customers, as well as by the general public. It is recommended that banking corporations avail themselves of outside specialists in the field, as necessary.

3.2 Based on the results of the assessment of risks, formulating a policy on the use the social media, including the type of information they will be used for, the types of social media that may be used, who in the banking corporation is responsible for publishing material via them, and the work processes and control mechanisms—and prescribing all these in the rules of the banking corporation.

3.3 Mapping out the banking corporation's uses, checking them against the results of the risks assessment and the policy, and making changes if and as necessary.

3.4 Taking account of the possibility of private uses of the social media by staff and customers of the banking corporation and their implications for the banking corporation's security system and controls.

3.5 Adopting controls to ensure that the policy and rules are being implemented (monitoring mechanisms, such as control of usage, and logs), and preparing procedures for responding to situations when a risk is realized.

3.6 Publishing directions and cautions to staff and customers.

3.7 Constant monitoring of trends, uses, risks and changes in the social media, so as to update and amend the policy, the rules and the methods of dealing with this matter.

Rony Hizkiyahu
Supervisor of Banks