November.
2016

GORNITZKY&CO

# Client Update: Regulators Impose New Cybersecurity Requirements on Financial Institutions*

In response to the increasing cybersecurity threats to the financial sector and considering the grave risks associated with such threats, regulators have introduced new cybersecurity requirements aimed at improving the protection of companies in the financial sector from such risks. This Client Update discusses two recent cybersecurity regulations that will affect financial institutions operating in the State of New York or in Israel – the proposed New York State Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies (the **"Proposed Regulation"**) and the Directive on the Management of Cyber Risks, published by the Israeli Ministry of Finance (the "**Israeli Directive**"). This Client Update also addresses guidelines recently issued by the Group of Seven Industrial Powers ("**G-7**").

On September 13, 2016, the NYDFS published the Proposed Regulation which requires financial institutions (such as banks and insurance companies) regulated by the NYDFS, to implement a number of measures to protect their systems from misuse, disruption and unauthorized access. Such measures include, inter alia, establishing and maintaining a cybersecurity program; adopting a cybersecurity policy which is to be reviewed on an annual basis by the board of directors and approved by a senior officer of such financial institution; appointing a chief information security officer who will be responsible for implementing and enforcing the cybersecurity program; adopting and implementing policies for

interactions with third parties (including the requirement of certain cyber-related representations and warranties from such third parties); and preparing a response and recovery plan for cybersecurity events.

Furthermore, the Proposed Regulation requires financial institutions to notify the superintendent of the NYDFS of cybersecurity events no later than 72 hours after becoming aware of the event, and to submit a certificate confirming compliance with the requirements under the Proposed Regulations to the superintendent on an annual basis.

Israel's financial regulators have also taken important steps to promote cyber readiness and resilience among companies operating in the Israeli financial sector. On August 31, 2016, following the March 2015 publication of the Bank of Israel's cybersecurity requirements applicable to banks and credit card companies, the Director of the Capital Market, Insurance and Savings Department in the Ministry of Finance of Israel issued the Israeli Directive, which applies to other financial institutions (such as insurance companies and companies managing provident funds and pension funds). The Israeli Directive imposes new requirements which are intended to promote the confidentiality, integrity and availability of sensitive information stored by such financial institutions, and to protect the proper function of their computer systems.

The Israeli Directive requires financial institutions to adopt a cybersecurity program and a policy which is to be approved by the board of directors on an annual basis; appoint a cybersecurity officer, who will oversee the cybersecurity program, implement a cybersecurity policy and guide the institution on cybersecurity in general; and to provide cybersecurity training to employees. Although the Israeli Directive requires financial institutions to notify the Ministry of Finance of cybersecurity events, in contrast to the NYDFS Proposed Regulation, it does not define a clear time frame for such notifications, but only states that such notifications shall be given "as soon as possible". The Israeli Directive also stipulates that the CEO of the financial institution shall be responsible for the management of the institution's cybersecurity risks and for allocating the proper resources in this regard.

Efforts to promote cybersecurity in the financial sector have also been made on an international level. On October 11, 2016, the G-7 issued a set of non-binding cybersecurity guidelines to promote cybersecurity best practices in the financial sector (titled G-7 Fundamental Elements of Cybersecurity for the Financial Sector). Such guidelines are intended to assist financial private and public entities in developing and shaping their cybersecurity strategy, in order to address the growing number of cyber threats. The G-7 guidelines consist of eight elements: establishing a cybersecurity strategy and framework; governance setting; conducting risk and control assessment; establishing monitoring processes; implementing response policies; establishing recovery plans; information sharing with internal and external stakeholders; and continuous learning.

The NYDFS Proposed Regulation is open for public comments until November 12, 2016. If adopted in its current proposed form, it would become effective on January 1, 2017. The Israeli Directive will become effective in Israel on April 2, 2017.

Gornitzky's Cyber-Security, Privacy and Data Protection team offers clients a well-rounded multidisciplinary approach to navigating the emerging regulatory and legal frameworks in the field of cyber security, privacy and data protection.

**For further information please contact:**


**Timor Belan,**
Partner
timorb@gornitzky.com
office: +972-3-7109191
fax: +972-3-5606555

**Assaf Harel,**
Associate
assafh@gornitzky.com
office: +972-3-7109191
fax: +972-3-5606555

**Shira Plotnik,**
Associate
shirapl@Gornitzky.com
office: +972-3-7109191
fax: +972-3-5606555


GORNITZKY&CO