/Carey

December 2020

NEW REGULATION ON INFORMATION SECURITY AND CYBERSECURITY FOR BANKS AND FINANCIAL INSTITUTIONS COMES INTO FORCE

On past December 1st, new chapter 20-10 of the Updated Regulations Compendium of the Financial Market Commission (the " **FMC** "), on information security and cybersecurity management, came into force (the " **New Rule** "), whose main provisions can be summarized as follows:

Regulatory scope

The New Rule is applicable to banks, their subsidiaries and supporting companies (sociedades de apoyo al giro), loans and savings cooperatives supervised by the FMC and payment cards issuers and operators (the " **Supervised Entities** "). [1]

Definitions

Considering the eminently technical character of this matter, the FMC has defined a series of concepts used throughout the New Rule, including "cyberspace", "cybersecurity", "cyber incident", "denial of services" and even "information".

General topics of management

The New Rule entrusts the Supervised Entities' board a key role on these matters, having the obligation to approve the institutional strategy, a proper budget for risk mitigation and the maintenance of a system for information security and cybersecurity management, as per the best existing international practices.

The New Rule sets, on a non-restrictive basis, a series of topics that shall be deemed as necessary for a proper management system of such aspects.

Risk management

The New Rule sets, as minimum guidelines on management of risks related to these matters, at least, the identification, assessment,

This news alert is provided by Carey y Cía. Ltda. for educational and informational purposes only and is not intended and should not be construed as legal advice.

Carey y Cía. Ltda.
Isidora Goyenechea 2800, 43rd Floor.
Las Condes, Santiago, Chile.
www.carey.cl

processing and acceptance or tolerance of risks the relevant entity's information assets are exposed to, as well as their permanent monitoring and review.

Specific elements for cybersecurity management

Considering their relevance, the New Rule particularly refers to two aspects that Supervised Entities shall consider in their management processes:

• The identification of the critical assets of the financial industry and the payment system, and the exchange of technical information on cybersecurity incidents with other members of this critical infrastructure, implementing policies for this purpose, and
• The response and recovery of the activities upon incidents.

This New Rule was enacted on July 6, 2020, after a public consultation process opened by the FMC.

---

[1] By mandate of: (i) Rule No. 8 of the FMC, for banks' subsidiaries; (ii) Rule No.3 of the FMC, for bank supporting companies; (iii) Rule No. 108 of the FMC, for loans and savings cooperatives supervised by the FMC, and (iv) Rule No. 2 of the FMC, for payment cards issuers and operators, respectively.

Authors: Felipe Moro; Fernando Noriega