مصرف لبنان
BANQUE DU LIBAN

Basic Circular No 144

Addressed to Banks and Financial Institutions

Attached is a copy of Basic Decision No 12725 of 28 November 2017 relating to Cybercrime Prevention.

Beirut, 28 November 2017

The Governor of Banque du Liban

Riad Toufic Salamé

Basic Decision No 12725

Cybercrime Prevention

The Governor of Banque du Liban,

Pursuant to the Code of Money and Credit, notably Articles 70, 174, and 182 thereof,

Pursuant to Law No 44 of 24 November 2015 (Fighting Money Laundering and Terrorist Financing),

Pursuant to Basic Decision No 7818 of 18 May 2001 and its amendments (Regulations on the Control of Financial and Banking Operations for Fighting Money Laundering and Terrorist Financing), attached to Basic Circular No 83,

Pursuant to the Cybercrime Prevention Guide issued jointly on 20 October 2016 by Banque du Liban, the Special Investigation Commission, the Association of Banks in Lebanon, and the Cybercrime and Intellectual Property Rights Bureau at the Judicial Police; and

Pursuant to the Decision of the Central Council of Banque du Liban, taken in its meeting of 21 November 2017,

Decides the following:

First: Cybercrime Prevention Policies and Procedures

Article 1: Banks and financial institutions must set policies and adopt measures and procedures relating to cybercrime prevention, and comprising at least:

I- General policies prescribing the following actions:

1- To analyze potential cybercrime risks, and to follow up the latest updates concerning cybersecurity technologies.

2- To allocate the necessary funds and budget in order to set and implement cybersecurity policy, systems, and rules.

3- To prepare insurance contracts that cover cybercrime risks.

4- To set and continuously update the plans needed for cybercrime prevention (e.g. incident response planning, disaster recovery and business continuity plan, first responder training plan…).

5- To create a task force for cybercrime prevention.

6- To exchange information on cybercrime with the concerned parties inside or outside the bank/financial institution.

7- To raise awareness among employees and customers regarding cybercrime prevention.

8- To monitor changes in employees' habits and behavior, particularly employees having elevated privileges to access IT systems.

9- To be vigilant and cautious when selecting contractors for tasks related to IT systems, and to make sure that these contractors do not in turn outsource these tasks to less reliable parties.

II- Technical procedures encompassing the following actions:

1- To adopt a minimum two-factor authentication technique, particularly to check the right of outside users to access the system of the bank/financial institution.

2- To use an end-to-end, high-grade encryption for crucial data, to avoid loss and tampering of such data.

3- To adopt tight rules for filtering incoming e-mails and for controlling external access to mailboxes.

4- To update the systems of all computers, and to check the safety of the computers assigned for the external use of the bank/financial institution's employees.

5- To carry on penetration tests to detect any possible vulnerabilities in the network.

6- To monitor the network traffic in order to detect any unusual behavior, whether through the quality or the number of sent batches.

7- To check and monitor data integrity, in order to detect any illegal tampering with data, and to trace back the source of the illegal access to such data.

Second: Financial Cybercrime Prevention Procedures

Article 2: As far as each is concerned, banks and financial institutions must adopt in general and on their own responsibility, the appropriate administrative, technical and judicial procedures which enable them to remain vigilant, to monitor and combat financial cybercrime. They must particularly:

1- Consider the guidelines specified in the Cybercrime Prevention Guide, Part 1, Section 1, as cybercrime indicators.

2- Adopt the Cybercrime Prevention Policies and Procedures specified in the Cybercrime Prevention Guide, Part 1, Section 2.

3- Set specific internal systems and procedures regarding the execution of funds transfer orders received electronically (through e-mail, e-banking, etc.)

4- To incorporate in the contract signed with the customer specific provisions that determine, apart from e-mail, other means of communication with the customer (such as phone calls), in order to validate transfer orders received electronically, provided any change in these means of communication takes place only through the contracting parties' written agreement.

5- To inform the customer of the risks associated with transfer orders sent through e-mail, to advise him/her to use safer means, and to obtain his/her risk-bearing written consent.

6- To provide the customer with the "Guidelines for Individuals and all other Non-Financial Institutions and Entities" specified in the Cybercrime Prevention Guide, Part 2.

7- To request from customers to promptly report any cybercrime, whenever they become aware or detect or are notified that they have been, or were likely to be, victims of a cybercrime.

Article 3: Banks and financial institutions are requested, whenever they detect or become aware or are notified that they have been the victims, or that any of their customers has been the victim of a financial cybercrime, to take prompt and effective actions that include, at least, the remedial measures mentioned in the Cybercrime Prevention Guide, Part 1, Section 3, particularly:

1- To provide both the correspondent bank and the beneficiary bank/financial institution with all relevant information, and to request the cancelling and the refund of the funds transfer.

2- To communicate to the Special Investigation Commission (SIC) any relevant information and correspondence, including technical information about:
   - The customer's IP address or the IP address used to send the suspicious funds transfer orders.
   - The name of the Internet Service Provider through which the suspicious funds transfer orders were sent.
   - The name of the Internet Service Provider used for the unauthorized access to the customer's account, through electronic banking.

3- To advise the customer to file a report or a judicial complaint before the competent authorities.

Article 4: The Compliance Department established at each bank and financial institution shall implement the provisions of this Decision.

Article 5: This Decision shall come into effect upon its issuance.

Article 6: This Decision shall be published in the Official Gazette.

Beirut, 28 November 2017
The Governor of Banque du Liban
Riad Toufic Salamé