Republic of Panama
Superintendency of Banks

RULE N.° 5-2021
(dated 23 November 2021)

"Whereby Article 15 of Rule 6-2011 is amended"

THE BOARD OF DIRECTORS
in use of its legal powers and,

WHEREAS:

Due to the issuance of Decree Law 2 dated 22 February 2008, the Executive Branch re-edited Decree Law 9 of 1998 and all its amendments as a consolidated text, and this text was approved by means of Executive Decree 52 dated 30 April 2008, hereinafter referred to as the Banking Law;

Pursuant to Article 5 (1) and (2) of the Banking Law, safeguarding the soundness and efficiency of the banking system and strengthening and fostering favorable conditions for the development of the Republic of Panama as an international financial center are objectives of the Superintendency of Banks;

Pursuant to Article 5 (3) and (4) of the Banking Law, promoting public trust in the banking system and safeguarding the judicial balance between the banking system and its clients are objectives of the Superintendency of Banks;

Pursuant to Article 11 (I)(5) of the Banking Law, establishing the administrative interpretation and scope of the legal provisions and regulations on banking matters is among the technical duties of the Board of Directors;

Rule 6-2011, amended by Rule 9-2014, established the guidelines on e-banking and related risk management;

In response to the growing national and international electronic frauds that constantly test the vulnerabilities of the electronic channels of the banking sector, the Superintendency has deemed it important to strengthen the guidelines on electronic banking, so that the services offered to customers are managed in a more secure, reliable and efficient manner in the banks in the market;

Taking into consideration the continuous technological changes, it is of vital importance for the Superintendency to ensure that banks adequately manage the risk related to the use of electronic channels that provide services to their clients, to ensure adequate protection of the banking client and, consequently, their electronic channel operations are conducted in a more secure and reliable manner;

During its working sessions, the Board of Directors determined it was necessary and advisable to update Article 15 of Rule 6-2011 to strengthen some guidelines in risk management of operations carried out by banks when the operations conducted by their clients, though their electronic banking channels, are exposed to growing electronic frauds.

RESOLVES:

ARTICLE 1. Article 15 (2) of Rule 6-2011 shall read:

"…

2. <u>Internet Banking and Mobile Banking</u>

At the Internet banking and mobile banking level, banks shall guarantee the implementation, as a minimum, of the following security measures:

a. Bank authentication. For the client to recognize the bank it will be necessary to have implemented, as a minimum, the following security measures:

a.1. A digital method (such as digital certificates, the client's preselected images or their equivalent) that will allow the client to verify he has the correct bank before the client enters his/her password.

a.2. Immediately after logging in, the full name of the client and the last date he/she entered the service must be shown for his/her verification.

b. Client authentication. To have access to this service it will be necessary to have the following authentication measures:

b.1. Category 1 authentication factor, which must meet the following parameters: generated first by the bank, with a possible subsequent modification by the client him/herself and containing at least eight (8) alphanumeric characters.

b.2. Category 2 authentication factor, which must meet the following parameters: implementation of a "dynamic validation" shield or a similar technology or processes that offers at least the same security level. This factor shall be applicable when a client makes transfers to a third party at the same or another bank.

In the case of dynamic validation, the bank must have an automated PIN generation system containing a minimum of six (6) digits.

Category 2 factor could be made either by hardware devices or portable software solutions inside mobile devices. This code shall be compulsory for carrying out bank transactions and optional for consultations made by the client through these channels.

PROVISO 1. For the purposes of the provisions of Article 15 (2(b)(b.2)) herein, banks must ensure that, for the activation process of the soft token, a secure client authentication process is carried out, for which the bank must ensure that it uses the most secure authentication mechanisms, such as, the hard token (category 2 factor) or category 3 factor and its derivatives with the highest level of certainty, signs of life, or others that may arise.

Likewise, for active internet banking and mobile banking clients, the bank must ensure that any changes related to the client information, such as changes to the telephone number, e-mail address, domicile, or other sensitive data, are considered within the bank's category 2 or category 3 authentication factor.

Banks will have up to 28 February 2022 to fully comply with the provisions established herein.

PROVISO 2. The bank that, as of the entry into force of this Rule, requests any authorization to implement new electronic channels or to add new services to a previously authorized channel, in compliance with the provisions of Article 3 herein, must comply with the requirements established in Proviso 1, as part of good electronic channels risk management.

Notwithstanding the foregoing, up to 28 February 2022 the Superintendency may authorize using any a channel or adding new services to a previously authorized channel, however, in these cases the bank must take the risks and incur in costs for transactions not recognized by its clients, as a consequence to the activation of the double authentication factor without the security measures provided in proviso 1 of this Article.

…”

ARTICLE 3. EFFECTIVE DATE. This Rule shall become effective upon its promulgation.

Given in Panama City on the twenty-third (23rd) day of November, two thousand twenty-one (2021).

FOR COMMUNICATION, PUBLICATION AND ENFORCEMENT.

THE CHAIRMAN, **THE SECRETARY,**

Luis Alberto La Rocca Rafael Guardia Pérez