

Republic of Panama Superintendency of Banks

**RULE N.º 2-2022
(dated 22 March 2022)**

“Whereby Article 15 of Rule 6-2011 is amended”

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

WHEREAS:

Pursuant to the issuance of Decree Law 2 dated 22 February 2008, the Executive Branch re-edited Decree Law 9 dated 26 February 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;

Pursuant to Rule 6-2011, amended by Rule 9-2014 and Rule 5-2021, the guidelines on e-banking and related risk management were established;

In response to the growing national and international electronic fraud that constantly tests the vulnerabilities of the banking sector's electronic channels, the Superintendency issued Rule 5-2021 to establish the requirements that allow the banks of the market to strengthen e-banking guidelines, so that the services offered to clients are provided in a more secure, reliable and efficient manner;

Rule 5-2021 set 28 February 2022 as the deadline for banks to make the necessary technological adjustments to comply with the requirements established in Proviso 1 of Article 15 (2) of Rule 6-2011;

By means of letter ABP/PE N.º 034-2022, the Panama Banking Association requested an extension to comply with the provisions included in Proviso 1 of Article 15 (2) of Rule 6-2011, so that banks may have an additional period to make the corresponding adjustments;

During its work sessions, the Board of Directors determined it was necessary and advisable to amend Article 15 of Rule 6-2011 to extend the deadline for compliance with the guidelines established in Proviso 1 of Article 15 (2).

RESOLVES:

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

“ ...

2. Internet Banking and Mobile Banking

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 authentication 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 a secure client authentication process is carried out, for the soft token activation process, 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 change related to the client information, such as changes to the telephone number, e-mail address, domicile, or other sensitive data, is considered within the bank's category 2 or category 3 authentication factor.

Banks will have up to 30 June 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 30 June 2022, the Superintendency may authorize using any 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 2. EFFECTIVE DATE. This Rule shall become effective upon its enactment.

Given at Panama City this twenty-second (22nd) day of March, two thousand twenty-two (2022).

FOR COMMUNICATION, PUBLICATION AND ENFORCEMENT.

THE CHAIRMAN,

THE SECRETARY,

Rafael Guardia Pérez

Felipe Echandi

