Republic of Panama
Superintendency of Banks

RULE No. 006-2011[1]
(dated 6 December 2011)

"Whereby the guidelines on E-banking and Related Risk Management are established"

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

CONSIDERING:

That due to the issuance of Decree Law 2 dated 22 February 2008, the Executive Branch reedited Decree Law 9 of 1998 and all of its amendments as a sole text, and that this text was approved by means of Executive Decree 52 dated 30 April 2008, hereinafter referred to as the Banking Law;

That, according to article 5 of the Banking Law the objectives of the Superintendency of Banks are to safeguard the soundness and efficiency of the banking system and to strengthen and foster favorable conditions for the development of the Republic of Panama as an international financial center;

That according to the provisions set forth in paragraph 3 of Article 5 of the Banking Law an objective of the Superintendency is to promote public trust in the banking system;

That according to the provisions set forth in Article 54 of the Banking Law banks shall have policies, regulations, and procedures assuring that their principal operations can be maintained or recovered in a timely manner in the event of any significant interruption that might affect their operational capability, in order to minimize the consequences that might arise from such an interruption;

That the constant emergence of new technologies and the transformation of existing ones pose numerous risks that require updating the regulatory framework for the provision of services through e-banking in order to ensure operations are carried out in a safer, transparent, reliable, and efficient manner;

That pursuant to the provisions set forth in Article 11 of the Banking Law and within the administrative sphere, establishing the interpretation and reach of the legal provisions and regulations on banking matters is among the technical duties of the Board of Directors;

That during the Board of Directors' working sessions it became obvious that it was necessary and advisable to update the parameters and guidelines for the provision of e-banking services in order to strengthen the management of risks to which these operations are exposed to through electronic media or channels:

RESOLVES:

ARTICLE 1: SCOPE OF APPLICATION. The provisions of this Rule shall be applicable to all state-owned, general license and international license banks providing or furnishing products to their clients through e-banking.

[1] Rescinded Rule 5-2003 dated 12 June 2003. Amended by Rule 9-2014 dated 24 September 2014.

ARTICLE 2: DEFINITIONS. For the purposes of this Rule, the following terms shall be understood as follows:

1. **E-banking:** Is the provision of banking services through electronic media or channels. E-banking includes the services offered by: internet banking, mobile banking, telephone banking, point of sale terminals (POS), instant messaging (chats), social networks, e-mail, e-signature, e-money, ACH networks, specialized networks, automatic teller machines, mobile wallet (smart card) or mobile payment, credit cards with a chip, e-payment means or any other electronic means or channel.

2. **Technological access device:** An element or component, whether hardware and/or software, that will allow a bank client to access e-banking services.

3. **Electronic media or channels:** Technological access devices, data transportation means, storage system or any other current or future technology that will be used to inquire, input, transport, protect, process and/or store clients' data and their banking transactions.

4. **Internet banking:** E-banking services provided to clients through internet, on the website belonging to one or more domains of the bank, through HTTP (Hypertext Transfer Protocol) or HTTPS (hypertext Transfer Protocol Secure) protocols or their equivalent, regardless of the technological access device.

5. **Mobile banking:** E-banking services provided to clients through a mobile phone, whose telephone number is affiliated to the service, through SMS (Short Message Service), WAP (Wireless Access Protocol) protocols or their equivalent.

6. **Telephone banking:** E-banking services whereby the client sends instructions to the bank through a telephone system, whether landline or mobile, through tones, pulses or voice recognition mechanisms, and the client receives a previously recorded answer or an interactive voice answer.

7. **Voice to voice telephone banking:** E-banking services whereby the client provides instructions through a telephone system, whether landline or mobile, to the bank by the intermediation of a representative authorized by the institution, located at a call center.

8. **Point of sale terminals:** Technological access devices allowing the provision of e-banking services, including dataphones, micro-computerized electronic terminals, mobile phones, and computer programs that could be operated by individuals or businesses to debit or credit bank accounts or apply charges to cards.

9. **Instant messaging:** Technological access means or channel whereby the client contacts a bank via internet or a similar system and in real time, and asks or provides information through a representative authorized by the institution.

10. **Social Networks:** Technological access means or channel whereby the client interacts with a bank via internet or a similar system or provides information through a representative authorized by the institution.

11. **E-mail:** Technological access means or channel whereby a client exchanges information with a bank through the internet and asks or provides information through a representative authorized by the institution.

12. **E-money:** Currency value of a bank account or another banking product accessed through electronic devices to make payments through point of sale terminals, direct transfer between two devices or through open computer networks.

13. **Automatic teller machine:** Technological access means that provides e-banking services that is accessed through a card and/or authentication procedures.

14. **Mobile wallet (smart card) or payment:** E-banking services in which the technological access device consists of an electronic device or the client's mobile phone, whose line is linked to the service.

15. **Bank card:** Technological access devices used as payment means (credit card, debit card, prepaid card and others).

16. **Card with a chip:** Credit cards with a chip that can store cardholder's information in order to verify, through cryptographic procedures, that the card and the point of sale where it is used are valid, before performing e-banking services.

17. **Specialized networks:** Information and/or funds transfer systems, whether domestic or international, between financial institutions and any other entity handling client information. This definition includes, among others, the system known as SWIFT.

18. **Authentication codes:** Authentication mechanisms based on information or devices that only the client knows and possesses or based on his physical characteristics, contained in the following categories:

    a. **Category 1 codes:** Information that only the client knows, such as his personal identification number, password or personal data voluntarily provided by him, through information and/or secure electronic channels.

    b. **Category 2 codes:** Information that only the client has, such as tokens, mobile phones, or bank cards with a chip or other security technologies that may emerge.

    c. **Category 3 codes:** Biometric information, such as fingerprints, hand geometry, iris features, etc.

ARTICLE 3: PRIOR AUTHORIZATION AND CONTROL FROM THE SUPERINTENDENCY. Banks may execute any e-banking service within or from the Republic of Panama, as long they have obtained prior authorization from the Superintendency of Banks for each electronic channel that the bank may want to implement. To that end, the bank shall provide the Superintendency of Banks complete information confirming the implementation and maintenance of the structures and measures contained herein.

Additionally, the bank may request an authorization from the Superintendency of Banks to incorporate new services to a previously authorized electronic channel, as provided for in the paragraph above. Notification to the Superintendency is required when the bank adds services of the same nature and structure to the ones previously approved.

Prior the service authorization, the Superintendency will carry out the inspections it deems advisable to verify, evaluate, and review the information furnished and the appropriate compliance with the provisions of this Rule.

Automatic teller machines, points of sale (POS) and, in general, technological access devices to be added to a bank's network will not require the authorization referred to in this article as long as these resources provide the same services through the same electronic channels previously authorized by the Superintendency. Without prejudice to the previous statement, the bank shall notify the Superintendency about the security measures that will be implemented for these channels prior to the installation of the equipment.

ARTICLE 4: RESPONSIBILITIES OF THE BOARD OF DIRECTORS AND TOP MANAGEMENT OF THE BANK. The board of directors and the top management of the bank shall be responsible for establishing and implementing an effective risk management system, especially for the risks involved in e-banking activities, including as a minimum:

1. The establishment of specific responsibilities, policies and controls for the ongoing analysis and management of these risks, including the establishment of a Responsible Unit and management by the Risks Committee.

2. The verification and approval of the basic aspects of the risk control process and the security of the bank's electronic channels.

3. The establishment of a comprehensive and continuous due diligence and supervision process for the handling of the bank's relationship with its external service providers and connections in general to third parties assisting or complementing e-banking.

ARTICLE 5: ADEQUATE E-BANKING STRUCTURE. The board of directors or top management of each bank must ensure that the bank's operations manual incorporates the necessary procedures, policies and internal controls to maintain an adequate administrative and operating structure for providing e-banking services, including particularly the following:

1. Nature of banking transactions and operations offered.

2. Transactions or operations registration system.

3. Effective mechanisms for the supervision of risk associated with e-banking activities (e.g. operational, technological, security risks, etc.) including, at a minimum, the establishment of policies and controls to manage such risks.

4. Effective mechanisms for evaluating threats, vulnerabilities and associated effects to the information files related to the process of e-banking.

5. Effective mechanisms for managing e-banking security threats and providing feedback to risk management.

6. Policies and procedures to be applied in case of potential internal and external security threats to e-banking, both to prevent them and to take the necessary actions when they occur.

7. Policies and procedures to be applied in case of internal and external security breaches to e-banking, including actions to be taken.

8. Policies and procedures including security mechanisms which include business continuity and disaster recovery plans.

9. Due diligence and vigilance mechanisms to manage outsourcing relationships related to e-banking services.

ARTICLE 6. BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS. The Risk Unit or the existing responsible unit in each bank shall have among its duties the development of a comprehensive plan both for business continuity and disaster recovery.

A business continuity plan is understood to be an operational interdisciplinary methodology consisting in various response plans to confront security contingencies or incidents that will allow the bank to immediately restore the critical functions that were partially or totally affected as a result of an attack, sabotage or natural disaster.

A disaster recovery plan is understood to be the process for recovery of data, communication links, critical hardware and software that have suffered an availability or security incident, permitting he bank to resume its normal functions and service.

ARTICLE 7. RESPONSIBLE UNITS. The risk unit or the existing responsible unit in each bank shall have among its duties the identification, evaluation, and control of technological risks, including risks associated to e-banking services.

For the daily management of information security, each bank shall have within its organizational structure an information security unit that will report to a senior, independent official.

Due to its organizational structure, a bank may request waivers to the above provisions from the Superintendency, as long as the bank shows to the satisfaction of the Superintendency that information security management is carried out efficiently by either its parent company or an outsourced security supplier.

ARTICLE 8: INTERNAL AUDIT. In regard to internal audits, the bank's responsibilities will be:

1. To ensure that periodic audits are carried out depending on the volume and sophistication of the bank's operations and to ensure these audits are incorporated into its Annual Audit Plan.
2. To have the necessary programs and specialized staff in the relevant areas.

ARTICLE 9: EXTERNAL AUDITS. The bank shall ensure that external risk audits of its e-banking channels and electronic payment means are carried out by qualified companies or personnel.

ARTICLE 10: PENETRATION AND VULNERABILITY TESTS. For the purpose of minimizing unauthorized access to their systems, all banks must undertake, as a minimum, the following penetration and vulnerability tests to be performed by qualified external professionals:

1. **External Security Penetration Test**:
   This test must be made at least once a year and shall inspect the following areas:

   a. Security devices and their functioning under attack.
   b. Vulnerabilities in web applications and internet banking.
   c. Evaluation of the intruder detection systems.
   d. Services open to public networks.
   e. Network structure.
   f. Failure in authentication systems and password policies.

g. Internal social engineering.

2. **Internal Security Penetration Test**:
   This test must be made at least every two (2) years and shall inspect the following areas:

   a. Analysis of network architecture and its topology.
   b. Identification of the critical information technology components.
   c. Identification of vulnerabilities and areas to be protected.
   d. Risk, incident, network and systems management.
   e. Physical and logical security.
   f. Incident management.

PARAGRAPH. Without prejudice of the provisions set forth in this article, the bank shall make penetration and vulnerability tests on a regular basis using its own qualified staff.

ARTICLE 11: COMPREHENSIVE MANAGEMENT OF RISKS ASSOCIATED WITH E-BANKING. All banks shall include within their comprehensive risk management processes the risks associated with the provision of services and products through e-banking, placing special attention on the management of operational, legal and reputational risks, as follows:

1. To ensure that the information provided or posted on their websites or through any electronic channel is suitable and will allow their clients to identify the bank adequately and correctly.

2. To ensure that the information provided or posted about the features of e-banking services and the minimum preventive measures that must be taken by the client, are correct and updated.

3. To establish technical measures and procedures to ensure the observance of privacy conditions applicable to clients and the security of their operations.

4. To adopt privacy measures applicable to the jurisdictions where the bank provides its products and services through any e-banking channel.

5. To establish programs that will guarantee the effectiveness and continuity of business ensuring the availability of e-banking services and systems.

6. To develop incident response and communication plans to manage, stop and mitigate problems that may arise from unexpected events, including internal and/or external attacks that may hinder the provision of e-banking services and systems.

7. To set up systems to manage cases of fraud related to e-banking services, including a comprehensive solution for the monitoring of client transactional behavior that contains methods of identification, early warning, preventive action, and investigatory follow-up for each case.

ARTICLE 12: RECORD OF E-BANKING ACCESS. The bank providing e-banking services shall establish and maintain the necessary logbooks, protected from manipulation and arbitrary alteration that will permit a clear audit track, with the date and time synchronized with Coordinated Universal Time.

The logbooks will include a record of system access and use indicating the transactions and operations carried out by clients. The bank will maintain the logbook at the disposal of the

Superintendency by any means authorized by Law, for a period not less than one (1) year, counted from the transaction date. The logbooks shall contain, at a minimum, the following information:

1. A record of access to electronic channels, including the client's identity, date and time.

2. A detail of the monetary operations made, including date, time, technological access channel, amount, origin account and destination account, and type of transaction (debit/credit).

3. The data that will allow investigations of electronic resources and/or channels, in order to facilitate finding the source of any fraud or attempt at fraud.

4. In the case of internet banking, storage of logbooks generated is required on the web server, and shall contain, as a minimum, the registration method (GET/POST/HEAD), the Uniform Resource Identifier (URI) and its parameters the time and date (timestamp).

The bank shall guarantee that e-banking services provided by third parties comply with the logbook requirements established in the paragraphs above and that both the bank and the Superintendency shall have access to them, if necessary.

ARTICLE 13: E-BANKING TRANSACTION RECORDS. The bank shall maintain a record of its clients' transactions as provided for in the Commercial Code.

ARTICLE 14: E-BANKING CONTRACT AND INFORMATION. The bank is required to inform the e-banking client about the features, conditions, potential costs and any other relevant stipulation the use of the e-banking service carries. This description must be specific and separate for each electronic resource or channel.

To this purpose, the bank must provide and include in its e-banking contract, the applicable information contained in Article 196 of the Banking Law for each electronic resource or channel making sure that the client knows the cost of e-banking services.

Also, it will be necessary to maintain evidence of the acceptance by the client of the terms and conditions applicable to each e-banking service.

ARTICLE 15: SECURITY CONTROLS. When providing e-banking series, the bank must ensure the authenticity, integrity and confidentiality of each transaction, must avoid the rejection of any valid transaction once it has been accepted, and must provide for the separation of authentication and control responsibilities. For this purpose, the bank shall have, as a minimum, the following:

1. **Technology Infrastructure**
   At the technology infrastructure level, banks shall guarantee the implementation of at least the following security measures:

Measure	Description
Application of secure ZONES by means of Firewall.	Banks shall have a Demilitarized Zone (DMZ) that isolates public services from the organization's internal network.
LOG Server.	There should be a server for storing the LOGS generated by the firewall (IP address, timestamp, event).

The implementation of an intruder detection system capable of working in active (IPS) or passive (IDS) form is required.	There should be an Intruder Detection System on the public side of the Demilitarized Zone (DMZ) that will analyze the traffic of the bank's public networks on the services posted on Internet. The logs generated by the system shall be stored for one (1) year. The program should be capable of generating statistics and summaries that can be requested by the Superintendency of Banks of Panama.

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 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 code, which must meet the following parameters: generated first by the bank, with a possible subsequent modification by the client himself and containing at least eight (8) alphanumeric characters.
b.2 Category 2 authentication code, which must meet the following parameters: implementation of a "dynamic validation" shield or a similar technology or process that offers at least the same security level. This code 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 automatic PIN system generating at least six (6) digits.

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

3. <u>Mobile Payment</u>

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

a. Identify the client by the mobile telephone number, which the bank must obtain automatically and clearly.

b. The Category 1 authentication code must have, at least four (4) characters.

c. Provide the necessary measures to prevent reading the identification and authentication information provided by the client on the screen of the access device.

d. Implement compensatory controls for protecting the transmission of the client sensitive information.

4. Automatic Teller Machines and Integrated Circuit Banking Cards[2]

At the automatic teller machine level, banks shall guarantee the implementation, as a minimum, of the following security measures:

a. Identify the client through the bank card number.

b. A Category one (1) authentication code whose password or personal identification number has at least four (4) digits and, additionally, an integrated circuit banking card.

c. If the automatic teller machine service is offered through regular banking cards (non-integrated circuit cards), banks must assume the risk and cost of operations not recognized by clients, while the balance of said transactions must be repaid to the client within seventy-two (72) hours after the claim has been filed, as long as the transaction was made by clients of a bank on the automatic teller machines of the same bank.

   In addition, if the transactions are made by the client on automatic teller machines of another bank of the market, the bank receiving the claim must pay the client the balance of the transactions within ten (10) days after the claim is filed.

   All banks in the Panamanian market must have integrated circuit banking cards within thirty-six (36) months after the promulgation of this Rule. However, the bank must have an implementation and operational plan within twenty-four (24) months after the promulgation of this Rule.

d. Provide the necessary measures to prevent the display of the identification and authentication information provided by the client on the access device screen.

e. Encrypted transmission of passwords, personal identification numbers and client's sensitive information.

f. Closed circuit television cameras (CCTV) and image recording, with the records being kept by the bank for a minimum of twelve (12) months. However, upon notification by competent authority, the bank must maintain the records at the disposal of the authorities for whatever period they may require.

PROVISO. Once the thirty-six (36) month period referred to in subparagraph c of this article has expired, banks that have not yet completed the distribution of the integrated circuit banking cards will have an additional three- (3) month period to complete the process.

Once the three- (3) month period in the previous paragraph has expired, those banks that have not yet completed the distribution of the integrated circuit banking cards to its clients may request a waiver from the Superintendent extending that period, explaining in detail the reasons that impede the bank meeting the deadlines herein. The Superintendent will evaluate the request for an extension, taking into account the card volume of each bank and the complexity of each particular case, and will decide how long an extension to grant based on the bank's justification.

[2] Amended by Article 1 of Rule 9-2014 dated 23 September 2014.

Nevertheless, as of 20 December 2014, the banks must assume all risks and cost of operations not recognized by clients that do not yet have access to the integrated circuit banking cards, as long as there is no negligence on the part of the client.

5. Point of sale terminals (POS)

At the point of sale terminal (POS) level, banks shall guarantee the implementation, as a minimum, of the following security measures:

a. Identify the client through a bank card number.

b. Category one (1) authentication code shall have at least four (4) digits when applicable to the card type, or banking card with a chip.

   In the event that the point of sale terminal services are offered through banking cards without a chip, the banks must assume the risk and cost of operations not recognized by clients, and the balance of said transactions must be repaid to the client within seventy-two (72) hours after the claim is filed. The bank must ensure that the point of sale terminals owned by third parties different from the bank have the security mechanisms required by this rule.

c. Provide the necessary measures to prevent on-screen reading on the access device of the identification and authentication information provided by the client.

d. Encrypted transmission of passwords, personal identification numbers or client's sensitive information.

e. The electronic device used as a point of sale terminal must meet the security measures established for e-payment processes.

6. Telephone Banking

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

a. Assign a unique client identifier, defined by the bank or by the client himself, containing at least six (6) characters.

b. A Category two (2) authentication code whose password or personal identification number contains at least six (6) digits. This code will be applicable when the client makes transfers to a third party at the same bank or another bank.

7. Voice-to-voice Telephone Banking

At the voice-to-voice telephone banking level, banks shall guarantee the implementation, as a minimum, of the following security measures:

a. Assign a unique client identifier, defined by the bank or by the client himself, containing at least six (6) characters.

b. A Category one (1) authentication code that has the information provided through questionnaires in call centers that will allow protection of the client's sensitive information.

8. Specialized networks

At the specialized network level, banks shall guarantee the implementation, as a minimum, of the following security measures:

1. Interaction of the parties:

   For e-banking services to be provided through specialized services networks, it will be necessary to have the following security measures:

   a. Both parties must use digital certificates and/or measures similar to those that identify and validate the legitimate source and content of the transaction.

   b. Encrypted links with the highest security levels commercially available shall be established.

   c. Bastion servers that will isolate and protect the bank's central information repositories must be used.

   d. Measures that guarantee the integrity and reliability of transactions and that will not reject or disavow valid transactions will be used.

9. Instant messaging, social networks and e-mails

At the instant messaging, social networks and email level, banks shall guarantee the provision of general information and any other information that has been authorized by a bank client in the contract or by any other means.

ARTICLE 16: OTHER E-BANKING CONTROLS. Besides the controls established in the previous article, the bank shall ensure implementation of the following e-banking controls in general:

a. Methods for the verification of identity and authorization of new clients, as well as the authentication of identity and authorization of existing clients wishing to initiate transactions through the e-banking service.

b. Measures established to preserve confidentiality and security of relevant bank information. These measures shall be proportionate to the sensitivity of the information transmitted and/or maintained in databases.

c. Techniques conducive to establishing the non-rejection or disavowal of information obtained and ensuring the confidentiality and integrity of e-banking transactions.

d. Provide confirmation of the execution of transactions made by the client through the service.

e. Methods for the separation of responsibilities, such as internal controls, to reduce the risk of fraud in operational processes and systems, and to ensure that transactions are duly authorized, registered and protected.

f. An adequate physical structure with corresponding controls will exist, such that all systems, servers, databases or physical information related to the e-banking service are protected and any unauthorized access will be detected.

g. Appropriate measures to ensure the accuracy of transactions through e-banking data records that may be transmitted through electronic channels or internet sites,

whether from internal databases of the bank or maintained by the bank's external service providers.

h. Ensure the implementation of adequate internal controls, particularly in cases and operations relevant to e-banking, such as:
h.1 An account opening, modification or closure.
h.2 Transactions carrying financial consequences.
h.3 Approved authorization for a client to exceed pre-established limits.
h.4 Approval, modification or revocation of rights or privileges to access the system.

i. Appropriate response plans to security incidents or the availability of information including communication strategies to ensure the continuity of the service and limited responsibility associated with interruptions of electronic banking services, including those originating from external systems. These plans and information must allow feedback for the risk management system in order to work on continual improvement of the effectiveness of applied controls and thereby reduce the risk assumed.

j. Adequate policies to ensure the appropriate assignment of responsibilities in case of irregularities in the use of e-banking services by third parties contracted for the implementation and execution of said service, through service quality agreements which clearing indicate the security controls that must be implemented by third parties.

k. Clear audit tracking for all e-banking transactions.

ARTICLE 17: REPORT OF SECURITY INCIDENTS. The bank shall report any event or fraud attempt to the e-banking services to the Superintendency of Banks using a form that will be provided for that purpose. This report must be submitted within the term established by the Superintendency, even though its source has not yet been determined, reporting, among others: the date and time, type, affected electronic means or channel, number of affected clients, estimated amount and other information requested in the relevant form.

ARTICLE 18: CLIENT INFORMATION PRIVACY AND SECURITY. The bank shall apply appropriate control techniques, such as cryptography, specific protocols or other controls, to guarantee the privacy and confidentiality of client information.

Appropriate measures shall be undertaken by the bank to inform e-banking clients regarding the management of security and privacy of information it collects. The following measures shall be established to that end:

a. Clearly inform the clients of the bank's policy on security for its e-banking service, where applicable.

b. Inform clients of the need to protect their password, personal identification number and any banking and personal information.

c. In the case of electronic banking via the Internet, once the client has introduced his password and accessed the "secure channel", the bank may not re-direct the user's session to other sites different from the site of the transaction and/or consultation without first informing the client that he is leaving the bank's site.

ARTICLE 19: RELATIONSHIP WITH THIRD PARTY E-BANKING AND SECURITY SERVICE PROVIDERS. When the bank hires the services of providers or third parties to execute e-banking services processes, prior authorization of the Superintendency of Banks will be required pursuant to the provisions of the Outsourcing Rule issued by the Superintendency. In case of a security provider, this provider shall have staff suitable to handling the services contracted.

Also, the information security providers shall be divided into the following categories:

a. Analysis, planning and implementation of information security management systems and/or logical monitoring solutions and security information management.

b. Auditors and certifiers.

For the services stated in subparagraph "a", the supplier providing the service cannot be the same executing the provisions stated in subparagraph "b" of this article.

ARTICLE 20: SUBMITTAL OF INFORMATION. Banks subject to this Rule shall submit to the Superintendency any information and reports related to e-banking services to be required by the Superintendency in the manner, timing and contents established by the Superintendency.

ARTICLE 21: PREVENTION OF THE IMPROPER USE OF E-BANKING. To prevent the improper use of e-banking services, the bank must ensure the existence and functioning of effective procedures and security measures for the identification and follow-up of suspicious transactions.

In this regard, the bank must apply the Know-Your-Client policy, due diligence procedures and other regulatory and legal provisions regarding the improper use of banking and trust services.

ARTICLE 22: SANCTIONS DUE TO NONCOMPLIANCE WITH THE RULE. Noncompliance with provisions contained in this Rule shall be sanctioned by the Superintendent pursuant to Title IV of the Banking Law.

ARTICLE 23: REPEAL. With the enactment of this Rule, the Rule 5-2003 dated 12 June 2003 shall be repealed.

ARTICLE 24:[3] This Rule shall become effective on the tenth (10^{th}) of September, two thousand twelve (2012). Notwithstanding the above:

a. Paragraph 7 of Article 11 shall become effective twenty-four (24) months after the promulgation of this Rule. However, within nine (9) months after the enactment of this Rule, all banks shall submit an action plan for the implementation of this paragraph.

b. The provisions in Paragraphs 2, 4, and 5 of Article 15 shall have a development period of twenty-four (24) months counted from the promulgation of this Rule, subject to the conditions and exceptions stated in the above paragraphs.

c. All banks shall have installed closed circuit television cameras technology within a thirty-six (36) month period, counted from the promulgation of this Rule. After this

[3] Amended by Article 2 of Rule 9-2014 dated 23 September 2014.

period, the bank may avail itself of an additional three- (3) month period, i.e. until 20 March 2015.

Given in the city of Panama, on the sixth (6th) day of December, two thousand eleven (2011).

LET IT BE KNOWN, PUBLISHED AND ENFORCED.

THE CHAIRMAN, **THE SECRETARY,**

Arturo Gerbaud De La Guardia Félix B. Maduro