RULE No. 01-2007[1]
(dated November 21, 2007)

"Whereby Minimum Security Standards are stipulated for the Banking Entities"

THE BOARD OF DIRECTORS
using its legal authority, and

WHEREAS:

Pursuant to Numeral 1 of Article 5 of Decree Law No. 9 of 1998, looking after the maintenance of the soundness and efficiency of the banking system is a function of the Superintendency of Banks;

Pursuant to Numeral 3 of Article 5 of Decree Law No. 9 of 1998, the Superintendency of Banks is responsible for promoting public confidence in the banking system;

By virtue of the increase of new criminal operating models perpetrated against the banking entities and the users of the banking premises, it is indispensable to implement minimum security measures so as to establish mechanisms and processes that help prevent accidents and criminal acts;

In work sessions of this Board of Directors with the Superintendent of Banks, the need and convenience has been made evident of setting the minimum security guidelines in banking entities to prevent and face the perpetration of illicit conducts and accidents, that attempt against the estate and the physical integrity of the banks' staff and customers, without inhibiting the growth of banking services.

RESOLVES:

ARTICLE 1: APPLICATION SCOPE. The provisions of this Rule will apply to Official Banks, General License Banks and International License Banks.

ARTICLE 2: SECURITY MEASURES FOR BANKS. In spite of the installation of those other security measures and protection it deems convenient and adequate, all banks must adopt in each establishment the following minimum security measures:

1. **General Security Measures in Banking Premises:**

    1.1 The banking entities must stipulate minimum security measures that include the installation and functioning of devices, mechanisms and equipment, aiming for the protection needed in the banking premises

[1] Paragraph 7.10 of Article 2 was amended by Rule 1-2012 dated 28 February 2012.

for customers, employees, public and property, setting parameters according to the establishment's location.

1.2 The provisions contained herein will be deemed as minimum measures, and therefore banking entities must at all times have security systems consistent with what is technically available at the moment.

1.3 All banking institutions will have secure areas and adequate and sufficient lighting. In places where cash is handled such as vaults, tellers, ATMs, drive-ins and night depositories, lighting and safety must be reinforced, ensuring also the permanent lighting of these places in case of an ultimate power outage.

1.4 The banking entities that provide customer service will keep controls of access to the premises.

1.5 The entrance doors to the bank must be equipped with two locks with coded keys or security keys, so that the presence of two persons is required at the time of opening and closing operations.

1.6 Banking entities must guard the inside and outside of their installations with private security guards, police agents or the bank's private security staff. "Outside" is understood as the surroundings of their installations, parking lots and public access that the bank has designated to be used by its staff and customers, even if they are a distance away from the bank's premises.

1.7 The access to the teller area must be restricted to the public, to the bank's non-authorized staff and must be located in such a way as to minimize the risk of third parties taking money.

1.8 It is explicitly forbidden for officers of the teller area to carry cellular phones, personal pagers or beepers. Communication means are allowed under the bank's control and supervision.

2. Manuals and Security and Protection Policies: Banking entities will have Manuals and Security and Protection Policies that must at least contain the following basic aspects for the institutions' safety, particularly of their employees and users, premises, goods and property, as well as for protection in transporting cash and valuables:

2.1 The policies, standards, principles and basic processes pursuant to which banking entities must formulate their security measures and protection.

2.2 The minimum security measures contained in this Rule, detailing their characteristics, and in case it applies, dimensions and quality of materials.

2.3 The other security measures that banking entities want to adopt in addition to those contained in this Rule.

2.4 The criteria for the design and construction of their premises, including the installation, functioning and control of devices, mechanisms, data processing and communication centers and technical protection team to provide the appropriate services.

2.5 The operating processes, systems and controls for preventing and detecting irregularities in executing their operations and in managing resources, cash and valuables they have under their responsibility.

2.6 The characteristics that the monitoring and alarm systems must meet, including the quality and availability indexes, as well as the other technical or technological characteristics necessary for effectively broadcasting and transmitting signals and images.

2.7 Aspects pertaining to information security, such as physical, logic, network and communication security, among others.

2.8 The criteria for the selection, recruitment and training of human resources, as well as for contracting professional services to provide security and protection to the premises.

2.9 The guidelines to grant the staff that works at the bank adequate training and information, specifically regarding training in case of accidents or during the perpetration of a crime, which should be updated at least once a year.

2.10 The devices, systems and procedures to monitor employees' entrance to and exit from the Bank.

2.11 The systems and procedures to monitor the entrance to and exit of customers, suppliers and others to the banking premises.

2.12 Procedures related to managing, safekeeping y guarding the information regarding the customers of the banking entities.

2.13 The bank's contingency and business continuity plans in case of accidents or criminal acts, whose effectiveness must be reviewed and tested at least once a year leaving written evidence.

3. Security Staff:

3.1 The banking entities will have employees that have the accountability of a Banking Security Officer's functions, who will have the task of directing, managing or coordinating the security program.

3.2 The banking entities must have security staff or agents that will safekeep the inside and outside of the bank's installations at the time the premises open, during the customer service schedule and as long as there are employees working. They will also be accountable for checking and inspecting customers, suppliers and others that enter. In this context, people can be directly or indirectly contracted by the bank to execute this function, or it can be done by private security agency staff.

3.3 In those cases where the banks hire private security agencies, the former must verify that the latter comply with the requirements stipulated by the Law that regulates the matter and the Ministry of Government and Justice.

3.4 Specific security functions will be assigned to the security staff or agent and never will they be assigned different functions.

4. Bank Vaults and Safes:

4.1 Vaults, safes and their nearby areas that contain cash and valuables will be given restricted access. They must have elements and systems that provide an adequate safety and protection, to its content as well as during the procedures of depositing and withdrawing cash and/or valuables that are object of transportation and protection.

4.2 The bank must comply with international standards for building vaults, safes and vault doors. In this context, they must comply with high security characteristics pursuant to the guidelines of American National Standard Institute or Underwriter Laboratories, Inc. They must also keep adequate insurance policies.

4.3 The doors of the bank vaults must have time clocks and ventilation systems. The vaults must have smoke sensors, movement and vibration sensors with strategically located panic buttons and communication systems.

4.4 The vaults will have outside and inside cameras.

4.5 The bank must set procedures for closing and opening vaults and for emergency situations – assault, accident or if a person remains inside after it is closed.

4.6 The safes and cash reserve holding compartments must have time clocks.

5. Theft and Fire Alarm Systems:

5.1 All the premises of the banking entities must have theft and fire alarm systems linked to monitoring systems and the latter must communicate with the Police or private Security Agencies and the Fire Brigade.

5.2 For theft risks the alarm systems must have the classification for banks, taking international standards into account.

5.3 Alarm systems must be periodically checked so as to prove that the equipment is working properly. Likewise, the communication systems must be checked with the police and security agency and in particular, with those in charge of security and protection and the top management officers.

5.4 At least once a year there must be a drill to test the operating system and the contingency plans in case of assault, theft, fire (with previous coordination with the Fire Brigade and Civil Protection), bomb threat, or other contingencies. A record must be kept of the periodic tests and drills carried out by the bank.

5.5 All alarms and other elements connected to the banking entity's security system must allow capturing, recording, broadcasting and transmitting in real time and simultaneously, the alarm signals as well as the crime or accident scenes.

6. Cameras:

6.1 The banking entities must at least have fixed or mobile Closed Circuit Television (CCTV) cameras with high resolution images (color camera, 1/3 color CCD image sensor, 480 line resolution, 0.8 lux minimum lighting, 24V voltage and digital recorder with 120 IPS recording speed), equipped with video recorders, hard disk or its equivalent in photographic cameras for taking instant pictures during 24 hours. The same must be tested monthly and posted in a logbook, so as to prove their proper functioning and the image neatness.

6.2 The banks must at least have fixed location cameras that adequately observe the places where the public and staff access the banking entity, the tellers that serve the public, the main door of the vault, the inside of the vault and ATMs.

6.3 The banks must have a tape file, a digital video disk (DVD) file or of any other recording system that covers at least three (3) months recording.

7. Automatic Teller Machines (ATMs): The banking institutions' ATMs must comply with the following measures:

7.1 Preventive Maintenance Program:

7.1.1 The banking institutions must develop a preventive maintenance program to ensure that all components in the Closed Circuit Television (CCTV) system and the image recording system of the ATM are clean and functioning according to the supplier/manufacturer's requirements.

7.1.2 They must ensure that the following minimum standards are kept in all ATM facilities:

7.1.2.1 The Closed Circuit Television (CCTV) cameras and the image recording cameras must be placed in such a way that a clear image of the individuals that enter the ATM installations can be obtained, avoiding recording the image of the person entering the PIN.

7.1.2.2 The Closed Circuit Television (CCTV) and the image recording systems must be maintained according to the supplier/manufacturer's recommendations.

7.1.2.3 They must have monitored alarm systems.

7.2 Closing Device (This does not apply to ATMs located in open areas):

7.2.1 The ATM facility access doors must have a mechanism that locks the door from the inside of the ATM facility.

7.3 Lighting:

7.3.1 The ATM area must be well lit, allowing the easy view from the inside of all persons at the entrance door and vice versa.

7.3.2 The lighting of the ATMs located in open areas must allow seeing all activities around it. Likewise, it must allow the effective functioning of the surveillance cameras.

7.4 Physical Inspections:

7.4.1 An inspection must be done regularly to make sure there are no foreign objects, devices or other uncommon mechanisms installed inside the ATM facility.

7.4.2 Similarly, the surveillance cameras must be inspected to know that they have not been manipulated.

7.5 Anchor Mechanism:

7.5.1 The ATMs must be secured to the floor with bolts or with another device that makes their removal difficult, except for those that are embedded to the wall.

7.6 ATM dashboard lock:

7.6.1 Any bank that acquires an ATM must request changing the lock located in its dashboard, which allows opening the door of all models.

7.7 Access to Supervisor Menu:

7.7.1 Implementing an access control to the supervisor menu, either through a password or some other effective mechanism that allows it to be activated from the time the ATM is installed. A policy to activate and periodically change the password must be established.

7.8 Set the adequate procedures to:

7.8.1 Periodically check the anchors, lighting, cameras and surroundings of the ATM

7.8.2 Supply the ATMs with money

7.8.3 Heed an alarm signal or accident signal

7.8.4 React to a power interruption

7.8.5 Train their own staff in daily ATM maintenance

7.9 Carry out educational campaigns for users about the use, location and pertinent security measures during the ATM’s use, including placing signs that allude to them in the ATM enclosures.

7.10 [2]Banks must have a tape file of digital video disks (DVD) or of any recording system covering at least twelve (12) months or recordings. Nevertheless, upon notification by competent authority, the bank must maintain the records at the disposal of the authorities for whatever period they may require.

PARAGRAPH: In case of ATMs installed in business premises, the bank will be responsible for guaranteeing due safety in said ATMs, including devices and procedures that allow identifying the user and the operations he performs, and recording images.

8. Transporting Funds and Valuables:

8.1 The receiving and sending of cash and valuables must be done in areas of restricted access to the public and by staff authorized by the institution, who must avoid risk exposure. These procedures must be included in the Security and Protection Manuals.

8.2 The transfer of funds and valuables must be done by duly authorized companies, using armored vehicles with adequate ventilation, communication systems and duly trained security staff. The banks must have their files up-to-date with the names, signatures and photographs of the company's staff that transports funds and valuables.

8.3 The company the bank hires to transport funds and valuables must have the necessary insurance policies to keep said funds safe in case of theft or other contingencies.

8.4 Those banks or bank establishments that require transporting funds and valuables on their own must do it in safety compartments, whose combination is only known by the bank staff in charge of receiving said funds and valuables. Furthermore, those funds and valuables must be accompanied by a security guard or police agent and two (2) bank officers. The funds and valuables must be delivered directly to the vaults and safes.

ARTICLE 3: CUSTOMIZING TIME PERIOD. The banking entities that at the time this Rule goes into effect do not have the security measures that totally satisfy the provisions set, will have a period of three (3) months to completely adjust to these rules.

ARTICLE 4: SANCTIONS. In case of breach of the provisions stipulated in this Rule, the sanctions stipulated in Article 137 of Decree Law No. 9 of 1998 will be applied.

---

[2] Amended by Rule 1-2012 dated 28 February 2012.

ARTICLE 5: EFFECT. This Rule will be in force from the time it is proclaimed.

Given in the City of Panama, on the twenty-first (21st) day of the month of November, two thousand seven (2007).