Republic of Panama

Superintendency of Banks

Agreement No. 5-2003
(of June 12, 2003)

THE BOARD OF DIRECTORS
In exercise of its legal faculties, and

WHEREAS:

The rapid development of online banking services involves both risks and benefits to the banks offering this service;

Pursuant to Law 43 of July 31, 2001, electronic documents and firms, electronic commerce certification entities, and the exchange of electronic documents are defined and regulated;

Pursuant to Circular No. 61 of November 6, 2000 and Circular No. 71-2000 of December 1, 2000 this Superintendency of Banks set forth basic requirements related to the supply of banking services via the Internet;

Pursuant to Law No. 42 of October 2, 2000 measures are established for the prevention of Money Laundering Crimes;

Pursuant to Number 1 of Article 5 of Decree Law No. 9 of 1998, the Superintendency is responsible for guaranteeing the strength and efficiency of the banking system;

Pursuant to Number 2 of Article 5 of Decree Law No. 9 of 1998, the Superintendency of Banks is responsible for strengthening and promoting auspicious conditions for the development of Panama as an international financial center;

Pursuant to Number 7 of Article 16 of Decree Law No. 9 of February 26, 1998, the Board of Directors is responsible for determining the interpretation and scope of legal and regulatory banking provisions in the administrative realm;

That in the course of joint work sessions of this Board of Directors and the Superintendency of Banks, there became evident the convenience of establishing basic guidelines relating to the exercise of electronic banking services, focused on the principle of technological neutrality, in an evolving market wherein services may be offered by various platforms and received via different media, as well as the supervision of banking services via Internet and other electronic media.

AGREES:

Article 1: **SCOPE OF APPLICATION.** The provisions of this Agreement shall apply to Official Banks, General License Banks, and to International License Banks providing electronic banking services to all their clients.

Article 2: DEFINITION OF ELECTRONIC BANKING. For the effects of this Agreement, electronic banking shall be understood to comprise any banking transaction made directly by the client via an electronic channel or Internet site.

NOTE: For the effects of this article, electronic banking involves all services offered via Internet, ACH net, automatic tellers or any other services accessed via electronic means.

Article 3: PRIOR AUTHORIZATION FROM THE SUPERINTENDENCY. Banks may offer electronic banking services in or from the Republic of Panama, contingent on such receiving prior authorization from the Superintendency of Banks.

To that end, the Bank shall provide the Superintendency of Banks complete information documenting the implementation, structure maintenance and measures as established in this Agreement.

Article 4: ADEQUATE STRUCTURE. The Board of Directors or Senior Management of each Bank undertaking the offer of electronic banking services shall delineate in their

Operations Manual the procedures, policies and internal controls necessary to maintain an adequate administrative and operative structure of electronic banking, especially the following:

a. Nature of banking transactions or operations offered.

b. Transactions or operations registration system.

c. Effective mechanisms for the supervision of risks associated with electronic banking, such as: operational, technological, security risks; to include, at a minimum, the establishment of policies and controls to manage such risks.

d. Security mechanisms, to include applicable policies and procedures for potential internal and external security threats, both preventive and corrective.

e. Due diligence and vigilance mechanisms to manage outsourcing and third party entities servicing the electronic banking system.

Article 5: RESPONSIBLE UNIT. The Bank's existing internal risk unit, established pursuant to Article 17 of Agreement 4-2001 of September 5, 2001, shall have among its responsibilities the identification, evaluation and control of risks associated to the electronic banking service.

Article 6: AUDITS. The Bank shall be responsible to permanently undertake periodic auditing of the evaluation, review and follow-up of electronic banking services operation, thereby requiring a Systems Auditor, internal or external, as well as the necessary software and specialized personnel in the pertinent areas.

Article 7: ELECTRONIC BANKING SERVICES. Following prior notification to the Superintendency of Banks, the Bank may offer the following services through electronic banking:

a. Questions and consultations regarding accounts, balances and banking rates.

b. Listing of transactions.

c. Send or receive messages from the Bank.

d. Access to the client's personal information to allow its modification or update.

e. Payments of loans, credit cards and other credit services.

f. Payment of public utilities.

g. Payments to certain private entities designated by the Bank.

h. Fund transfers between accounts of the same bank.

i. Reporting loss of credit or debit cards issued by the Bank.

j. Requests for loan approvals.

Evidence of electronic banking contract acceptance shall be necessary, without requiring the conventional signature. A website link to the general conditions is required to manifest their existence, and to make them easily accessible on the screen and printed.

Article 10: SECURITY CONTROLS. Banks shall ensure the authenticity of all transactions, the integrity of the information transmitted, the confidentiality, their non-release or rejection once accepted, the separation of responsibilities and authorization controls. For these purposes, the system must possess, as a minimum:

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

b. Measures established to preserve confidentiality and security of the bank's relevant information, which shall be proportionate to the sensitivity of the information transmitted and/or maintained in data bases.

c. Techniques conducive to establishing the non-disclosure or rejection of the information obtained and to ensure the confidentiality and integrity of electronic banking transactions.

d. 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.

e. There shall exist an adequate physical structure with corresponding controls, such that all systems, servers, data bases or physical information related to the electronic banking service are protected and any unauthorized access may be detected.

f. Appropriate measures to ensure the accuracy, completion and trustworthiness of all transactions and data registers related to electronic banking that may be transmitted through an electronic channel or Internet site, whether from internal data bases of the Bank or maintained by the Bank's external service providers.

g. Ensure the implementation of adequate internal controls, particularly in cases and operations relevant to electronic banking, such as:

g.1. An account opening, modification or closure.

g.2. Transactions carrying financial consequences.

g.3. Approved authorization to a client to exceed pre-established limits.

g.4. Approval, modification or revocation of rights or privileges to access the system.

h. Appropriate response plans to incidents, to include communications strategies to ensure the continuity of the service and limited responsibility associated to interruptions of electronic banking services, including those originating from external systems.

i. Adequate policies ensure the appropriate assignment of responsibilities in case of irregularities in the use of electronic banking services by third party entities contracted for the implementation of said service.

Article 11: INTERACTION WITH ELECTRONIC BANKING SERVICE PROVIDERS. Upon contracting the implementation and maintenance of electronic banking services, the Bank shall ensure that the contractor has applied due diligence insofar as the aforementioned measures, and shall verify that such contractor has the necessary financial strength, reputation, policies and risk management controls, and the ability to comply with its obligations.

Article 12: CLIENT INFORMATION PRIVACY AND SECURITY. The Bank shall apply appropriate control techniques, such as cryptography, specific protocols or other controls to guarantee privacy and confidentiality of client information.

Appropriate measures shall be undertaken by the Bank to inform electronic banking clients regarding the management of security and privacy of the information gathered. The following measures shall be established to that end:

a. Clearly inform the clients of the Bank's policy on security for its electronic banking service, where applicable.

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

c. Inform clients of electronic banking via Internet that once their password or code has been introduced and they access the 'secure channel', their transactions and consults shall be limited to those permitted within that channel.

Article 13: PREVENTION OF THE INAPPROPRIATE USE OF ELECTRONIC BANKING. To prevent the improper use of banking services through electronic banking

services, the Bank shall ensure the existence, effectiveness and functioning of strict and efficient security procedures and measures for the identification and follow-up of suspicious transactions, as well as the application of the Know-Your-Client policy, Due Diligence procedures and other regulatory provisions contained in Agreement 9-2000 of October 23, 2000 and any other legal requirements establishing measures for the prevention of Money Laundering Crimes.

Article 14: IMPLEMENTATION OF LAW 43 OF JULY 31, 2001. Applicable provisions pursuant to Law 43 of July 31, 2001 shall be applied as they concern electronic documents.

Article 15: **SANCTIONS DUE TO NONCOMPLIANCE WITH THE AGREEMENT.** Noncompliance with provisions contained in this Agreement shall be sanctioned by the Superintendency pursuant to Article 137 of Decree Law No. 9 of 1998.

Article 16: **EFFECT.** This agreement shall become effective upon its promulgation.

Article 17: IMPLEMENTATION TERM. Banks shall have an implementation term of six months as of the date of promulgation, to comply with the provisions set forth in this Agreement.

Given in the city of Panama, on the twelfth (12th) day of the month of June two thousand three (2003).

COMMUNICATE, PUBLISH AND ENFORCE:

THE PRESIDENT **THE SECRETARY**