#2004-22
(amends EA #2003-33)

UNITED STATES OF AMERICA
DEPARTMENT OF THE TREASURY
OFFICE OF THE COMPTROLLER OF THE CURRENCY

AMENDMENT TO THE FORMAL AGREEMENT

The Comptroller of the Currency of the United States of America ("Comptroller"), through his National Bank Examiner, has examined Industrial Bank, N.A., Washington, D.C. ("Bank"), and his findings are contained in the Report of Examination for the examination that commenced on October 6, 2003 ("ROE").

The Bank, by and through its duly elected and acting Board of Directors ("Board"), has agreed to a Formal Agreement, executed on April 21, 2003 ("Agreement"). This amendment to the Agreement ("Amendment") supplements the Agreement. All jurisdiction and general provisions of the Agreement shall apply to this Amendment. The Agreement and this Amendment shall continue in full force and effect unless or until such provisions are excepted, waived, or terminated in writing by the Comptroller. It is agreed between the Bank, by and through its duly elected and acting Board of Directors, and the Comptroller, through his authorized representative, that the Bank shall operate at all times in compliance with the articles of the Agreement and this Amendment.

All reports or plans that the Bank or Board has agreed to submit to the Assistant Deputy Comptroller pursuant to this Amendment shall be forwarded to:

John W. Quill, Assistant Deputy Comptroller
Maryland/National Capital Field Office
Mail Stop 3-5
250 E. Street, S.W.
Washington, D.C. 20219-0001

ARTICLE IX

INFORMATION TECHNOLOGY

(1) For purposes of this Amendment, "Information Technology" (IT) means all systems and methods by or through which the Bank processes data and information, including mainframe computer systems, personal or microcomputers, telecommunication networks, and Internet banking servers, whether maintained by the Bank or a third-party.

(2) For purposes of this Amendment, "Internet banking" (IB) includes systems that enable individuals to access general information on the Bank's products and services or through which Bank customers may communicate or transact business with the Bank, through a personal computer or other intelligent device.

(3) Within ninety (90) days, the Bank shall develop and implement effective IT and IB security and operations policies and procedures as described in the Federal Financial Institutions Examination Council's most recent version of the Information Systems Examination Handbook; and other relevant OCC guidance, including: OCC Bulletin 97-23, FFIEC Interagency Statement on Corporate Business Resumption and Contingency Planning; OCC Bulletin 98-3, Technology Risk Management; OCC Bulletin 98-38, Technology Risk Management - PC Banking; OCC Bulletin 2000-14, Infrastructure Threats - Intrusion Risks; OCC Bulletin 2001-8, Guidelines Establishing Standards for Safeguarding Customer Information; OCC Bulletin 2001-47, Third-party Relationships – Risk Management Principals; OCC Advisory Letter 2000-9, Third-Party Risk; and OCC Advisory Letter 2000-12 - FFIEC Guidance on Risk Management of Outsourced Technology Services. These policies and procedures shall address, at a minimum:

(a) logical and physical security, including customer privacy considerations, of all IT equipment;

(b) appropriate periodic testing of security controls to identify whether system security has been compromised;

(c) appropriate staff training to ensure familiarity with the Bank's IT and IB policies and procedures;

(d) minimum due diligence standards for the selection and monitoring of third-party vendors.

(4) The Bank shall initiate all steps necessary to improve the management of Information Technology (IT) activities, including Internet banking (IB) activities. Within thirty (30) days, the Bank shall enact each corrective action listed under the "Immediate Tactical Corrections" section of this Article and, within one hundred and eighty (180) days, enact each corrective action listed under the "Strategic Corrections" section of this Article. Also, management and the Board should ensure that all corrective actions documented in the June 2003 IB Letter to the Board are addressed. Specifically, management should perform the following:

(a) Immediate Tactical Corrections

(i) specify employees (by position) who should have "administrative" access to the Bank's systems, including the purpose for such access; reduce administrative access to only those employees and establish a system to control and monitor administrative access;

(ii) specify employees (by position) who should have Internet access, including the purpose for such access; reduce Internet access to

only those employees and establish a system to control and monitor Internet access;

(iii) determine the cause and correct the problem of Bank emails received by unintended parties and document the rationale for re-implementing the outsourced email server;

(iv) ensure all appropriate risks are documented and internal controls are implemented prior to bringing the email server in-house;

(v) conduct an assessment of customer and Bank information within the Bank and at Fiserv to validate the integrity;

(vi) refrain from implementing any new electronic banking or IT activities until current issues are resolved;

(b) Strategic Corrections

(i) obtain the expertise to identify, measure, monitor and control IT risks within the Bank;

(ii) once this requisite expertise is obtained, this person(s) needs to prepare a formal risk assessment to identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

(iii) additionally, this person(s) needs to complete a business impact analysis (BIA) to identify the potential impact of uncontrolled, non-specific events on the Bank's business processes and customers. Consider all departments and business functions, not

just data processing, and estimate the maximum allowable downtime and acceptable levels of data, operations, and financial losses;

(iv) develop a formal action plan to prioritize and correct issues from the October 2003 IT internal audit and other third-party reports. The plan should focus on short-term and long-term steps and include specific timeframes for completion of the plan;

(v) designate a member of senior management to maintain responsibility and accountability for the timely completion of the action plan;

(vi) enhance the Information Security Program to comply with section 501b of the Gramm Leach Bliley Act (GLBA).

(5) Upon completion of the Immediate Tactical Corrections and the Strategic Corrections, respectively, a copy of the documentation of each action shall be submitted to the Assistant Deputy Comptroller for review.

(6) The Board shall ensure that the Bank has processes, personnel, and control systems to ensure implementation of and adherence to the program developed pursuant to this Article.

ARTICLE X

INFORMATION TECHNOLOGY RESUMPTION AND CONTINGENCY PLAN

(1) Within one hundred and eighty (180) days, the Bank shall develop and test a formal Disaster Recovery Plan (Plan) to ensure prompt resumption of services in the case of a disaster. The Bank shall ensure the plan complies with the Federal Financial Institutions Examination Council (FFIEC) Interagency Statement on Corporate Business Resumption and Contingency Planning, OCC 97-23, and the FFIEC's Information Systems Examination Handbook guidance on developing an organization-wide contingency plan.

(2) Within one-hundred and eighty (180) days, and at least annually thereafter, the Board shall review its IT resumption and contingency planning and perform a test of all necessary programs and system applications using its backup location, or recovery operation center, to ensure the continuation of operations in the event of a disaster. The Board shall document the results of this review and test in its meeting minutes.

(3) A copy of the Plan shall be forwarded to the Assistant Deputy Comptroller for review.

(4) The Board shall ensure that the Bank has processes, personnel, and control systems to ensure the development and implementation of and adherence to the policies, procedures, programs, and testing required pursuant to this Article.

ARTICLE XI

THIRD-PARTY RISK MANAGEMENT

(1) Effective immediately, before the Bank enters into a contractual agreement with any third-party vendor that provides material services to the Bank (i.e., those for which management spends over $75,000 annually, or those deemed critical to the Bank's operations), the Board shall perform a comprehensive review of management's due diligence review of the third-party. The due diligence should involve a thorough evaluation of all available information about the third-party, including qualitative and quantitative aspects, both financial and operational, and assess whether the third-party can help the Bank achieve its strategic goals.

(2) Effectively immediately, for all new or renewed third-party relationships, the Board and management, depending on amount and criticality, should ensure that the expectations and obligations of the vendor and the Bank are clearly defined, understood, and enforceable. The following topics should be considered when entering into a binding contract or agreement (some points may not apply in every circumstance). Documentation supporting the rationale concluding that any of the following is not included in a vendor contract should be maintained.

(a) Scope of arrangement, including the use, if any, of subcontractors.

(b) Performance measures or benchmarks.

(c) Responsibilities for providing and receiving information.

(d) The right to audit.

(e) Cost and compensation.

(f) Ownership and license.

(g) Confidentiality and security.

(h) Business resumption and contingency plans.

(i) Indemnification.

(j) Insurance.

(k) Dispute resolution.

(l) Limits on liability.

(m) Default and termination.

(n) Customer Complaints.

(o) OCC Supervision.

(3) Within ninety (90) days, the Board shall designate a Bank officer with sufficient expertise to monitor all material third-party relationships with respect to their activities and performance. The oversight program should monitor the third-party's financial condition, its controls, and the quality of its service and support. Performance monitoring should include at a minimum:

(a) Monitoring the Financial Condition - Evaluate the third-party's financial condition at least annually, and more frequently when financial indicators begin to deteriorate. This analysis should be as comprehensive as the ongoing credit analysis the Bank would conduct of its borrowers. Audited financial statements should be required for significant relationships with third parties;

(b) Monitoring Controls - Review audit reports (e.g., internal audits, external audits, SAS 70 reviews, security reviews), as well as examination reports, if available. Follow up on any deficiencies noted. Review the third-party's business resumption contingency planning and testing to ensure that all Bank services can be restored within an acceptable time. For many

critical services, annual or more frequent tests of the contingency plan are typical. Review any results of those tests and ensure that recovery times meet Bank requirements. Documentation of the above reviews should be maintained by Bank management;

(c) Assessing the Quality of Service and Support - Regularly review reports documenting the third-party's performance relative to service-level agreements. Determine whether contractual terms and conditions are being met, and whether any revisions to service-level agreements or other terms are needed.

In the event that the above analysis demonstrates any third-party has failed to provide acceptable services to the Bank or to maintain the necessary management, staff, controls, procedures and information systems, and if such third-party is unable or unwilling to correct these deficiencies, the Board shall terminate the contract between the Bank and the third-party.

(4) Within ninety (90) days, management and the Board must properly document its third-party oversight program. Proper documentation will facilitate the monitoring and management of the risks associated with third-party relationships. Proper documentation should include:

(a) A list of significant third-parties, i.e., those for which management spends substantial amounts of money, or those deemed critical to the operation;

(b) Valid, current, and complete contracts;

(c) Business plans for new lines of business or products that identify management's planning process, decision making, and due diligence in selecting a third-party;

(d) Regular risk management and performance reports received from the third-party (for example, audit reports, security reviews, reports indicating compliance with service-level agreements); and

(e) Regular reports to the Board, or a delegated committee, of the results of the ongoing oversight activities.

(5) Upon completion of the Third-Party Risk Management Plan, including the above monitoring and documentation requirements, a copy of the Plan and all documentation shall be submitted to the Assistant Deputy Comptroller for review.

(6) The Board shall ensure that the Bank has processes, personnel, and control systems to ensure the development and implementation of and adherence to the policies, procedures, programs, and testing required pursuant to this Article.

IN TESTIMONY WHEREOF, the undersigned, authorized by the Comptroller, has hereunto set his hand on behalf of the Comptroller.

/S/ *John W. Quill* *3/22/04*

John W. Quill
Assistant Deputy Comptroller
Washington, D.C. Field Office

Date

IN TESTIMONY WHEREOF, the undersigned, as the duly elected and acting Board of Directors of the Bank, have hereunto set their hands on behalf of the Bank.

Signed	3-22-04
Clinton W. Chapman, Esq., Chairman	Date
Signed	3/22/04
Massie S. Fleming	Date
Signed	
Robert R. Hagans	Date
Benjamin L. King, CPA	Date
Cynthia T. Mitchell	Date
Signed	3/22/04
B. Doyle Mitchell, Jr.	Date
Signed	3/22/04
Pamela King Smith	Date
Signed	3/22/04
Emerson A. Williams, M.D.	Date