

## **SUPERVISORY AGREEMENT**

This Supervisory Agreement (Agreement) is made this 10<sup>th</sup> day of September, by and through the Board of Directors (Board) of Sunshine Savings Bank, Tallahassee, Florida, OTS Docket No. 17971 (Association) and the Office of Thrift Supervision (OTS), acting by and through its Regional Director for the Southeast Region (Regional Director);

**WHEREAS**, the OTS, pursuant to 12 U.S.C. § 1818, has the statutory authority to enter into and enforce supervisory agreements to ensure the establishment and maintenance of appropriate safeguards in the operation of the entities it regulates; and

**WHEREAS**, the Association is subject to examination, regulation and supervision by the OTS; and

**WHEREAS**, based on its examination and regulatory oversight of the Association, the OTS finds that the Association has engaged in unsafe or unsound practices and/or violations of law or regulation; and

**WHEREAS**, in furtherance of their common goal to ensure that the Association addresses the unsafe or unsound practices and/or violations of law or regulation identified by the OTS in the May 3, 2010 Report of Examination (ROE), the Association and the OTS have mutually agreed to enter into this Agreement; and

**WHEREAS**, on September 9, 2010, the Association's Board, at a duly constituted meeting, adopted a resolution (Board Resolution) that authorizes the Association to enter into this Agreement and directs compliance by the Association and its directors, officers, employees, and other institution-affiliated parties with each and every provision of this Agreement.

**NOW THEREFORE**, in consideration of the above premises, it is agreed as follows:

**Information Technology Management.**

1. Within sixty (60) days, the Association shall retain a qualified manager for the Association's Information Technology (IT) operations whose responsibilities shall include, but not be limited to, managing and directing the Association's in-house core processing system, risk assessment processes and procedures, information security program, business continuity planning, and all other IT management functions.

**Information Technology Audit.**

2. Within sixty (60) days, the Association shall develop and adhere to an audit program that complies with applicable law, regulation and regulatory guidance and addresses all corrective actions in the 2010 ROE (IT Audit Program). The IT Audit Program shall include a detailed risk assessment process and development of comprehensive audit procedures.

3. Effective immediately, the Association's IT audit contracts shall comply with all contract language requirements discussed in the Interagency Guidelines Establishing Information Security Standards (Security Guidelines). The IT audit contracts shall include procedures and processes to meet the objectives and requirements of the Security Guidelines.

**Business Continuity.**

4. Within sixty (60) days, the Association shall revise its Business Continuity Program to include procedures, processes and systems to ensure that the Association's Business Continuity Program practices are reviewed and assessed by an internal and external party for compliance with applicable law, regulation and regulatory guidance within sixty (60) days after the end of each calendar year, beginning with the year 2010, or immediately following a significant software change or update.

5. Within sixty (60) days, the Association shall conduct a test of its disaster recovery site's suitability to serve as a recovery center, including a determination that the storage location for backup tapes is sufficiently remote to protect the tapes from a single disaster impacting both the service center and the storage facility. Thereafter, the Association shall conduct a test of its hot site's suitability to serve as a recovery center by September 30 of each calendar year, beginning with the year 2010, or immediately following a significant software change or update.

6. Within sixty (60) days, the Association shall conduct a Business Impact Analysis (BIA) and related business continuity risk assessment to ensure that both are current for the Association's operating environment. Thereafter, the Association shall conduct a BIA and business continuity risk assessment within sixty (60) days after the end of each calendar year, beginning with the calendar year 2011.

**Information Security.**

7. Effective immediately, the Association's information security risk assessments shall comply with applicable law, regulation and regulatory guidance and address all corrective actions in the 2010 ROE.

8. Effective immediately, the Association shall prohibit all remote access by employees to Association data and computer systems until adequate procedures, controls and requirements governing such access have been developed and implemented consistent with Paragraph 10 of this Agreement.

9. Within thirty (30) days, the Association shall designate or retain a qualified person to manage and administer the Association's information security program (Security Program).

10. Within sixty (60) days, the Association shall revise its Information Security Standards and Procedures and Information Security Policy ("Security Policies") and Security Program and

develop additional procedures, systems and controls to address all corrective actions related to information security discussed in the 2010 ROE. The Security Policies and Security Program shall, at a minimum:

- (a) establish processes and controls, including annual review by the Board, to ensure that the Association's information security risk assessment, Security Policies and Security Program comply with applicable law, regulation and regulatory guidance;
- (b) establish access controls and a periodic review process to ensure that access to the Association's information systems and IT applications, including the FedLine Advantage System, is restricted to current employees with a demonstrated need for access based upon job duties, functions, and responsibilities;
- (c) require and provide for the security and encryption of backup data that will be maintained offsite to reduce risks related to loss in transit or breach of the off-site storage facility;
- (d) require annual reports to the Board detailing the Association's compliance with its Security Policies and Security Program, including reports detailing the results of any third party reviews;
- (e) establish detailed procedures and controls over remote access of the Association's internal data and computer systems by employees; and
- (f) require annual training of all employees on information security, including the Association's Security Policies and Security Program.

11. Within sixty (60) days, the Association shall develop and adhere to procedures, processes and controls for responding to security tests performed by third party consultants (Third Party Review Procedures). The Third Party Review Procedures shall include detailed processes and

systems for reviewing third party reports, including third party security test reports, monitoring the completion of all recommendations within a reasonable period of time, and documentation of the review of all third party test reports and completion of all recommended corrective actions.

**Vendor and Technology Management.**

12. Effective immediately, the Association shall comply with its Vendor Management Program Policy. Within sixty (60) days, the Association shall address all areas of noncompliance with its Vendor Management Program Policy discussed in the 2010 ROE by risk rating its existing service providers, conducting due diligence on all third party service providers consistent with the Association's Vendor Management Program Policy, and fully documenting the risk rating of its service providers and due diligence that was conducted by the Association in the Association's books and records.

13. Within sixty (60) days, the Association shall develop a written plan and process for evaluating and meeting the Association's technology needs, including the acquisition and/or updating of all hardware and software (Technology Plan). The Technology Plan shall, at a minimum, include:

- (a) a comprehensive risk assessment process to identify the Association's areas of risk, technology needs, and outstanding software updates that apply to the Association's IT environment;
- (b) an assessment of identified risks, technology needs and outstanding software updates, including the Fiserv Premier software, and prioritization of and completion dates for all technology needs and software updates by degree of criticality;
- (c) a review of application controls and security concerns prior to entering into a contract with any third party service provider.

- (d) a testing process for Fiserv Premier core applications utilized by the Association that will include the ability to test recommended changes prior to implementation; and
- (e) analysis and planning for training of Association employees for newly acquired or updated technology or software.

**Pandemic Plan Testing.**

14. Within sixty (60) days, the Association shall conduct a test of its pandemic plan that addresses all corrective actions in the 2010 ROE and complies with applicable law, regulation and regulatory requirements. Thereafter, the Association shall test its Pandemic Plan on a periodic basis, but not less than sixty (60) days after the end of each calendar year, beginning with the calendar year 2011.

**Computer Room Environment.**

15. Within sixty (60) days, the Association shall address all corrective actions in the 2010 ROE related to the condition and working environment of the Association's technology operations computer room.

**Effective Date.**

16. This Agreement is effective on the Effective Date as shown on the first page.

**Duration.**

17. This Agreement shall remain in effect until terminated, modified or suspended, by written notice of such action by the OTS, acting by and through its authorized representatives.

**Time Calculations.**

18. Calculation of time limitations for compliance with the terms of this Agreement run from the Effective Date and shall be based on calendar days, unless otherwise noted.

### **Submissions and Notices**

19. All submissions to the OTS that are required by or contemplated by the Agreement shall be submitted within the specified timeframes.

20. Except as otherwise provided herein, all submissions, requests, communications, consents or other documents relating to this Agreement shall be in writing and sent by first class U.S. mail (or by reputable overnight carrier, electronic facsimile transmission or hand delivery by messenger) addressed as follows:

- (a) To the OTS:  
Regional Director  
Office of Thrift Supervision  
1475 Peachtree St., N.E.  
Atlanta, Georgia 30309  
404.897.1861 (Fax)
  
- (b) To the Association:  
Board of Directors  
c/o Jack Madden, Chairman  
Sunshine Savings Bank  
1400 East Park Avenue  
Tallahassee, FL 32301

### **No Violations Authorized.**

21. Nothing in this Agreement shall be construed as allowing the Association, its Board, officers or employees to violate any law, rule, or regulation.

### **OTS Authority Not Affected.**

22. Nothing in this Agreement shall inhibit, estop, bar or otherwise prevent the OTS from taking any other action affecting the Association if at any time the OTS deems it appropriate to do so to fulfill the responsibilities placed upon the OTS by law.

**Other Governmental Actions Not Affected.**

23. The Association acknowledges and agrees that its execution of the Agreement is solely for the purpose of resolving the matters addressed herein, consistent with Paragraph 23 above, and does not otherwise release, discharge, compromise, settle, dismiss, resolve, or in any way affect any actions, charges against, or liability of the Association that arise pursuant to this action or otherwise, and that may be or have been brought by any governmental entity other than the OTS.

**Miscellaneous.**

24. The laws of the United States of America shall govern the construction and validity of this Agreement.

25. If any provision of this Agreement is ruled to be invalid, illegal, or unenforceable by the decision of any Court of competent jurisdiction, the validity, legality, and enforceability of the remaining provisions hereof shall not in any way be affected or impaired thereby, unless the Regional Director in his or her sole discretion determines otherwise.

26. All references to the OTS in this Agreement shall also mean any of the OTS's predecessors, successors, and assigns.

27. The section and paragraph headings in this Agreement are for convenience only and shall not affect the interpretation of this Agreement.

28. The terms of this Agreement represent the final agreement of the parties with respect to the subject matters thereof, and constitute the sole agreement of the parties with respect to such subject matters.



**Enforceability of Agreement.**

29. This Agreement is a “written agreement” entered into with an agency within the meaning and for the purposes of 12 U.S.C. § 1818.

**Signature of Directors/Board Resolution.**

30. Each Director signing this Agreement attests that he or she voted in favor of a Board Resolution authorizing the consent of the Association to the issuance and execution of the Agreement. This Agreement may be executed in counterparts by the directors after approval of execution of the Agreement at a duly called board meeting. A copy of the Board Resolution authorizing execution of this Agreement shall be delivered to the OTS, along with the executed original(s) of this Agreement.

**[Remainder of Page Intentionally Left Blank]**

**WHEREFORE**, the OTS, acting by and through its Regional Director, and the Board of the Association, hereby execute this Agreement.

**SUNSHINE SAVINGS BANK**  
Tallahassee, Florida

**OFFICE OF THRIFT SUPERVISION**

/s/  
By: \_\_\_\_\_  
Jack W. Madden, Chairman

/s/  
By: \_\_\_\_\_  
James G. Price  
Regional Director, Southeast Region

**BOARD OF DIRECTORS SIGNATURES**

/s/  
\_\_\_\_\_  
Ben F. Betts, Jr., Director

/s/  
\_\_\_\_\_  
Jack P. Dodd, Director

/s/  
\_\_\_\_\_  
Louis O. Davis, Jr., Director

/s/  
\_\_\_\_\_  
Patrick E. Lyons, Director

/s/  
\_\_\_\_\_  
Brian P. Baggett, Director

/s/  
\_\_\_\_\_  
Doris K. Richter, Director