FEDERAL DEPOSIT INSURANCE CORPORATION
WASHINGTON, D.C.

and

SOUTH CAROLINA
BOARD OF FINANCIAL INSTITUTIONS
COLUMBIA, SOUTH CAROLINA

In the Matter of COMMUNITY FIRST BANK, INC. WALHALLA, SOUTH CAROLINA (Insured State Nonmember Bank)	)	CONSENT ORDER FDIC-14-0393b

The Federal Deposit Insurance Corporation ("FDIC") is the appropriate Federal banking agency for Community First Bank, Inc., Walhalla, South Carolina ("Bank"), under section 3(q) of the Federal Deposit Insurance Act ("Act"), 12 U.S.C. § 1813(q).

The Bank, by and through its duly elected and acting Board of Directors ("Board"), has executed a "STIPULATION AND CONSENT TO THE ISSUANCE OF A CONSENT ORDER" ("CONSENT AGREEMENT"), dated January 15, 2015, that is accepted by the FDIC and the Commissioner of Banking on behalf of the South Carolina Board of Financial Institutions ("State Board"). With the CONSENT AGREEMENT, the Bank has consented, without admitting or denying any charges of unsafe or unsound banking practices or violations of law or regulation relating to weaknesses in information technology ("IT"), to the issuance of this Consent Order ("ORDER") by the FDIC and the State Board.

Having determined that the requirements for issuance of an order under section 8(b) of the Act, 12 U.S.C. § 1818(b), and S.C. Code Ann. § 34-1-60 have been satisfied, the FDIC and the State Board hereby order that:

INFORMATION TECHNOLOGY

1. (a) Within 60 days from the effective date of this ORDER, the Bank shall develop, and the Board shall review, a comprehensive IT Plan ("IT Plan") for the safe and sound operation of the Bank's information technology assets, including, but not limited to, software, operating procedures, facilities, and the protection of accurate Bank records. The IT Plan shall be consistent with the Federal Financial Institutions Examination Council's ("FFIEC") *Information Technology Examination Handbooks*, http://ithandbook.ffiec.gov/. At a minimum, such IT Plan shall provide for:

(i) development and implementation of the ongoing internal and external IT audit programs required by Paragraph 2 of this ORDER;

(ii) strategies for mitigating risks, appropriate information security controls, employee training requirements, appropriate segregation of duties, and review of users' access to the IT area;

(iii) prompt Board review of all audits and regulatory report exceptions regarding the Bank's IT and written recordation of corrective responses of the Board to such exceptions;

(iv) an annual review of the Bank's IT Plan and its implementation, by the Board;

(v) independent testing of all key controls for IT including all IT systems designated as high or medium risk, and the retention of testing documentation;

(vi) an annual update of the IT risk assessment and vendor management risk assessments and retention of risk assessment documentation;

(vii) formal internal security monitoring policies and procedures for the network and other critical platforms specifying the necessary reports, exception criteria, requirements for documentation and reporting, events to monitor, assignment of appropriate responsibilities, specific requirements for documentation, and the reporting and follow up of exceptions;

(viii) formal project management policy to support all IT projects including project budgeting, testing, completion time frames, security, quality assurance guidelines and review process, and management reporting;

(ix) procedures for documenting requests for significant changes to the Bank's hardware and software and requests for changes to in-house parameters and the appropriate segregation of duties throughout the change management process; and

(x) recovery time objectives in the Business Impact Analysis incorporating the guidance provided in the FFIEC IT *Booklet on Business Continuity Planning.*

(b) Within 60 days from the effective date of this ORDER, the IT Plan shall be submitted to the Supervisory Authorities for review and comment. Within 30 days from receipt by the Bank of the Supervisory Authorities' written responses to the IT Plan, and after consideration by the Board of the comments from the Supervisory Authorities, if any, the Board shall adopt, and the Bank shall implement, such IT Plan.

(c) Within 60 days from the effective date of this ORDER, the Bank shall appoint an Information Security Officer with the requisite skills, knowledge, independence, and expertise, responsible for overseeing the development, implementation, and maintenance of the Bank's Information Security Program. This individual shall be empowered with sufficient authority and

independence as well as provided with sufficient training in information security to perform the duties required and ensure compliance with the guidelines of 12 C.F.R. Part 364-Appendix B.

(d) Within 90 days from the effective date of this ORDER, the Board shall conduct a review of staffing to ensure that adequate IT resources are provided for in terms of the number of employees as well as required skills, knowledge, and experience. IT personnel shall have experience in the technology systems and platforms deployed by the Bank.

(e) Within 90 days from the effective date of this ORDER, the Bank shall complete a written risk assessment of its IT functions to identify and mitigate threats and risks to IT assets and customer data from both internal and external sources. The written risk assessment shall be conducted in conformance with 12 C.F.R. Part 364-Appendix B, and as prescribed in the FFIEC IT *Booklet on Information Security*. The written risk assessment shall include, at a minimum, the following:

(i) identification of Board members, committee members, or other designees charged with overseeing the risk assessment process;

(ii) identification of threats and risks by area, including internal control weaknesses and conflicting duties;

(iii) identification of the likelihood or probability of such threats, taking into consideration natural, intentional, and unintentional causes;

(iv) methods for mitigating or minimizing threats and risks through administrative, technical, or physical controls; and

(v) reports to the Board of high and medium IT risks identified in the risk assessment.

(f) Beginning on the effective date of this ORDER, the Board shall increase its involvement and oversight of IT and document the Board's oversight activities in the minutes of

the meetings of the Board. The Board minutes shall thoroughly document items discussed and all determinations made on IT matters.

(g) Within 90 days from the effective date of this ORDER, the Board shall revise its formal written IT Strategic Plan to identify all short and long-term goals and the allocation of IT resources to achieve them. The IT Strategic Plan shall address the minimum factors detailed in the FFIEC IT *Booklet on Management* including, but not limited to budgeting, periodic Board reporting, sufficiency of IT staffing, goals for the IT audit function, and the status of the risk management controls supporting IT.

(h) Within 60 days from the effective date of this ORDER, the Bank shall develop adequate written policies and procedures covering electronic funds transfer activity including proper controls and segregation of duties, contracts with vendors, automatic clearing house ("ACH") audit, and wire transfer activity. The Bank shall review the policies and procedures annually and any recommended modifications or enhancements shall be presented to the Board for approval. The policies and procedures for electronic funds transfer activity shall be acceptable to the Supervisory Authorities as determined by subsequent examinations or visitations.

(i) Within 60 days from the effective date of this ORDER, the Bank shall develop and implement a written plan to correct all IT deficiencies identified in the Report of Examination dated May 12, 2014 ("Report").

IT AUDIT

2. (a) Within 45 days from the effective date of this ORDER, the Bank shall develop a written IT Audit Program that provides for comprehensive and ongoing audit coverage of all technology platforms. The IT Audit Program shall provide for a separate annual audit of the Bank's ACH and wire transfer functions. The IT Audit Program shall include the minimum

requirements detailed in the FFIEC IT *Booklet on Audit*. The scope and frequency of audits shall be governed by the Bank's enterprise-wide risk assessment where the controls identified shall be independently tested to evaluate if controls are working as intended, and remain effective over time. The IT Audit Program shall also provide for a tracking system to monitor exceptions through timely resolution that identifies, among other items, the responsible party and the expected remedy date.

(b) Within 30 days from the effective date of this ORDER, the Bank shall retain a qualified independent firm acceptable to the Supervisory Authorities to perform an external audit of the IT Plan which shall include a penetration test, vulnerability assessment, evaluation of the Bank's compliance with the information security standards of 12 C.F.R. Part 364-Appendix B, information security controls, IT general controls, and electronic funds transfer systems. The Bank shall provide a copy of the scope of the IT audit to the Supervisory Authorities within 10 days of the Bank's receipt of the scope of the audit.

(c) Within 120 days from the effective date of this ORDER, the Bank shall complete the external IT audit. The external IT audit report shall be presented to the Board for review, with the review noted in the Board minutes. The Bank shall develop, and the Board shall approve, a plan to address any exceptions identified in the external IT audit. The Bank shall provide a copy of the external IT audit to the Supervisory Authorities within 10 days of the Bank's receipt of the audit.

SHAREHOLDER DISCLOSURE

3. Within 30 days from the effective date of this ORDER, the Bank shall send a copy of this ORDER, or otherwise furnish a description of this ORDER, to its parent holding company. The description shall fully describe this ORDER in all material respects.

PROGRESS REPORTS

4. During the life of this ORDER, the Bank shall furnish written progress reports to the Supervisory Authorities within 30 days from the end of each quarter, detailing the form and manner of any actions taken to secure compliance with this ORDER and the results thereof. Such reports may be discontinued when the corrections required by this ORDER have been accomplished and the Supervisory Authorities have released the Bank in writing from making further reports. All progress reports and other written responses to this ORDER shall be reviewed by the Board and made a part of the appropriate Board meeting minutes.

The provisions of this ORDER shall not bar, estop, or otherwise prevent the FDIC, the Commissioner or any other federal or state agency or department from taking any other action against the Bank or any of the Bank's current or former institution-affiliated parties.

This ORDER shall be effective on the date of issuance.

The provisions of this ORDER shall be binding upon the Bank, its institution-affiliated parties, and any successors and assigns thereof.

The provisions of this ORDER shall remain effective and enforceable except to the extent that and until such time as any provision has been modified, terminated, suspended, or set aside in writing.

Issued Pursuant to Delegated Authority.

Dated: January 16, 2015

By:

/s/

Michael J. Dean
Regional Director
Division of Risk Management Supervision
Federal Deposit Insurance Corporation

The Commissioner, having duly approved the foregoing ORDER on behalf of the State Board, and the Bank, through its Board, agree that the issuance of said ORDER by the FDIC shall be binding as between the Bank and the State Board to the same degree and to the same legal effect that such ORDER would be binding if the State Board had issued a separate ORDER that included and incorporated all of the provisions of the foregoing ORDER, pursuant to S.C. Code Ann. § 34-1-60 (1976).

Dated: 1-15-15

By:

/s/

_____

Louie A. Jacobs
Commissioner of Banking
South Carolina Board of Financial Institutions