FEDERAL DEPOSIT INSURANCE CORPORATION
WASHINGTON, D.C.

In the Matter of	)	
COMMUNITY BANK AND TRUST – ALABAMA UNION SPRINGS, ALABAMA	)	CONSENT ORDER
(INSURED STATE NONMEMBER BANK)	)	FDIC-14-0310b

The Federal Deposit Insurance Corporation ("FDIC") is the appropriate Federal banking agency for Community Bank and Trust – Alabama, Union Springs, Alabama ("Bank"), under 12 U.S.C. § 1813(q).

The Bank, by and through its duly elected and acting Board of Directors ("Board"), has executed a "Stipulation to the Issuance of a Consent Order" ("STIPULATION"), dated January 28, 2015, that is accepted by the FDIC and the Alabama State Banking Department ("Department"). The Department may issue an order pursuant to Section 5-2A-12 of the Code of Alabama. With the STIPULATION, the Bank has consented, without admitting or denying any charges of unsafe or unsound banking practices or violations of law or regulation, to the issuance of this Consent Order ("ORDER") by the FDIC and the Department.

Having determined that the requirements for the issuance of an order under section 8(b) of the Federal Deposit Insurance Act ("the Act"), 12 U.S.C. § 1818(b), and Section 5-2A-12 of the Code of Alabama have been satisfied, the FDIC and the Department hereby order that:

BOARD OF DIRECTORS

1. (a) As of the effective date of this ORDER, the Board shall increase its participation in the affairs of the Bank, assuming full responsibility for the approval of sound Information Technology (IT) policies and objectives and for the supervision of all of the Bank's IT activities, consistent with the role and expertise commonly expected for directors of banks of comparable size. At each Board meeting, participation shall include, at a minimum, the following areas which should be reviewed and approved: audit reports; internal control reviews including management's responses; any significant changes to the IT infrastructure; reports from the Business Continuity Planning/Disaster Recovery ("BCP/DR") Coordinator; and compliance with this ORDER. Board meeting minutes shall document these reviews and approvals, including the names of any dissenting directors.

(b) Within 30 days from the effective date of this ORDER, the Board shall establish a Board committee ("Compliance Committee"), consisting of all outside Board members and the Chief Executive Officer, charged with the responsibility of ensuring that the Bank complies with the provisions of this ORDER, overseeing corrective measures with respect to the ORDER, and reporting to the Board. Bank management shall provide the Compliance Committee with monthly reports detailing the Bank's actions with respect to compliance with the ORDER. The Compliance Committee shall present a report detailing the Bank's adherence to this ORDER to the Board at each regularly scheduled Board meeting. Such report and any discussion shall be recorded in the minutes of the Board's meetings and shall be retained in the Bank's records. Nothing contained herein shall diminish the responsibility of the entire Board to ensure compliance with the provisions of this ORDER.

(c) 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. At a minimum, the IT Strategic Plan shall address the factors detailed in the FFIEC (Federal Financial Institution Examination Council) IT *Booklet on Management* including, but not limited to, budgeting, periodic Board reporting, sufficiency of IT staffing, goals for the IT audit function, the status of the risk management controls supporting IT, and contingency planning for the replacement of IT functions and services should an unexpected interruptions or loss of services occur.

(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 Board shall review all IT policies and procedures to ensure that they sufficiently address all relevant areas detailed in the FFIEC IT Handbooks applicable to the Bank. These policies and procedures shall be reviewed by management annually for necessary modifications and presented to the Board for annual approval.

MANAGEMENT

2. (a) The Bank shall have and retain management qualified to oversee all aspects of the Bank's IT operations, including compliance with all applicable IT laws and regulations.

(b) Within 30 days from the effective date of this ORDER, the Board shall appoint a qualified IT Manager responsible for managing the Bank's IT infrastructure.

VENDOR MANAGEMENT PROGRAM

3. (a) Within 30 days from the effective date of this ORDER, the Bank shall designate a Vendor Management Coordinator with an appropriate level of due diligence and vendor risk modeling experience for the type and quality of the Bank's IT services. The Vendor Management Coordinator shall be vested with sufficient authority to fulfill the duties and responsibilities of the position and shall report directly to the Board or the Compliance Committee.

(b) Within 90 days from the effective date of this ORDER, the Bank shall develop a written Vendor Management Program that meets the requirements and guidance of the FFIEC IT Examination Handbook, *Outsourcing Technology Services*, and provides a comprehensive inventory, assessment, and ongoing evaluation of all service providers. At a minimum, the Bank shall ensure that service providers with access to non-public customer information comply with the requirements of FDIC Rules and Regulations Part 364, Appendix B: *Interagency Guidelines Establishing Information Security Standards* ("Part 364"); and the Bank shall review all service providers in accordance with the level of risk posed to the Bank by the service provider's access to the Bank's customer information, which shall include, but is not be limited to, a review of the service provider's financial condition, security audits of the service providers, a review of regulatory reports prepared by the regulators of the service providers, if any, and adequacy of the service providers' BCP/DR plans to ensure that they meet the Part 364 requirements. The Vendor Management Program shall also include: the identity of all vendors with access to non-public customer information; detailed due diligence procedures for selecting a vendor; a vendor risk assessment model and associated definitions; risk-based policies to control and monitor outsourcing actions; due diligence and contract negotiation; implementation and service level

agreement procedures; and monitoring procedures that identify and evaluate changes in the risk from previous assessments. The Vendor Management Program shall be submitted to the Regional Director of the FDIC's Atlanta Regional Office ("Regional Director") and to the Superintendent of the Department ("Superintendent") (collectively the "Supervisory Authorities") for non-objection or comment.

Within 30 days of receipt of non-objection or any comments from the Supervisory Authorities, the Board shall approve, adopt, and implement the written individualized Vendor Management Program, and such approval shall be recorded in the minutes of the Board meeting. Thereafter, the Bank shall test and update the written individualized Vendor Management Program at least annually.

(c) Within 60 days from the effective date of this ORDER, the Bank shall determine the viability of the continued use of all IT Service Providers, including the Bank's primary IT Service Provider. Board meeting minutes shall document the review and approval or disapproval of the continued use of all IT Service Providers, including its primary IT Service Provider. The Board shall document the names of any dissenting directors.

BUSINESS CONTINUITY PLANNING /DISASTER RECOVERY PROGRAM

4. (a) Within 30 days from the effective date of this ORDER, the Bank shall designate a BCP/DR Coordinator with experience in contingency planning, testing, and coordinating. The BCP/DR Coordinator shall be granted sufficient authority to fulfill the duties and responsibilities of the position and shall report to the Board or the Compliance Committee.

(b) Within 60 days from the effective date of this ORDER, the Bank shall develop a written BCP/DR Plan that incorporates the guidance provided in the FFIEC's IT Examination

Handbook, *Business Continuity Planning*. The BCP/DR Plan shall be submitted to the "Supervisory Authorities" for non-objection or comment.

(i) The Bank's BCP/DR Plan shall include a disaster recovery testing program that identifies roles and responsibilities; a testing policy that includes testing strategies and test planning; the execution, evaluation, independent assessment, and reporting of test results; and updates to the BCP/DR program as needed.

(ii) The BCP/DR Plan shall include a written enterprise-wide Business Impact Analysis ("BIA") that assesses the sudden loss of IT services and incorporates the guidance provided in the FFIEC IT Examination Handbook, *Business Continuity Planning*. Thereafter, as part of the required annual BCP/DR testing, the Bank shall validate the BIA Recovery Time Objectives and Recovery Point Objectives. In addition the Bank shall update the BIA at least annually and include significant changes to the IT infrastructure. Results of the BIA shall be reported to the Board, which shall be noted in the minutes of the Board meeting. The BIA shall, at a minimum, include: a list of all IT functions and services that are currently provided by all IT Service Providers; the impact on the Bank for each service provided to include the potential of and priority of recovery; and the maximum acceptable recovery/replacement time for each service provided by all IT Service Providers.

(c) Within 30 days of receipt of non-objection or any comments from the Supervisory Authorities, the Board shall approve, adopt and implement the BCP/DR Plan, and such approval shall be recorded in the minutes of the Board meeting. Thereafter, the Bank shall test and update the BCP/DR Plan at least annually. Results of the test shall be reported to the Board, which shall be noted in the minutes of the Board meeting.

AUDIT PROGRAM

5. (a) Within 60 days from the effective date of this ORDER, the Bank shall develop a written IT Audit Program that provides comprehensive and ongoing audit coverage and submit the program to the Supervisory Authorities for non-objection or comment. The IT Audit Program shall provide comprehensive and ongoing audit coverage, and the scope of the program shall be enterprise-wide. The IT Audit Program shall include the areas recommended in the FFIEC IT Examination Handbook, *Audit* Booklet, including, but not limited to, a scoring system that risk rates significant business units, departments, and product lines; an audit schedule and cycles to test controls based on the IT Risk Assessment; the resources to be allocated for the audit; and provisions for regularly recurring assessment and updating of the IT Audit Program. All audit reports shall be written and submitted to the Board for review, which shall be noted in the minutes of the Board meeting.

(b) Within 30 days from receipt of non-objection or any comments from the Supervisory Authorities, and after incorporation and adoption of all comments, the Board shall approve and implement the IT Audit Program, and such approval shall be recorded in the minutes of the Board meeting. Thereafter, the Bank shall implement and fully comply with the IT Audit Program.

(c) Within 180 days from the effective date of this ORDER, the Bank shall have undergone a comprehensive IT audit. The IT audit shall be performed by independent auditors/IT security professionals with qualified experience and expertise in IT. As used in this section, the term independent shall have the meaning provided in the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. At a

minimum, the IT audit shall include compliance with the information security standards set forth at 12 C.F.R. Part 364 - Appendix B, information security controls, IT general controls, and electronic funds transfer systems. Thereafter, IT Audits shall be performed at least annually with written reports presented to the Board for review, which shall be noted in the minutes of the Board meeting.

(d) Within 30 days from the effective date of this ORDER, the Bank shall develop, adopt, and implement a tracking system for all IT audit and examination deficiencies that includes the source of the deficiency, corrective action promised, the person responsible for the corrective action, and the date by which corrective action is due. The Bank's internal auditor shall report on all outstanding deficiencies at each meeting of the Audit Committee and deficiencies cleared since the previous meeting, for the Bank's audit findings as well as for all IT Service Provider audit findings.

INFORMATION SECURITY PROGRAM

6. (a) Within 90 days from the effective date of this ORDER, the Bank shall develop a Board-approved Information Security Program (ISP) that includes the elements set forth in Part 364 Appendix B of the FDIC's Rules and Regulations. The ISP shall include, at a minimum, assigned responsibilities, a comprehensive information security risk assessment, adequate written policies and procedures, employee security awareness training, annual independent testing, oversight of service providers, a method for adjusting the program as necessary, and an annual review by the Board of compliance with the Information Security Program.

(b) Within 90 days from the effective date of this ORDER, the ISP shall be submitted to the Supervisory Authorities for review and comment. Within 30 days from the Bank's receipt

of the Supervisory Authorities' written responses to the ISP, and after incorporation and adoption of all comments, if any, the Board shall amend as necessary, approve, adopt, and implement the ISP, and such approval shall be recorded in the minutes of the Board meeting.

(c) Within 30 days from the effective date of this ORDER, the Board shall formally appoint an Information Security Officer (ISO), with the requisite skills, knowledge, and expertise, necessary to oversee the development, implementation, and maintenance of the ISP. This individual shall be empowered with sufficient authority and independence and provided with sufficient external training in Information Security to perform the duties required and ensure compliance with the guidelines of Part 364 Appendix B of the FDIC's Rules and Regulations. The ISO shall report to the Board or the Compliance Committee.

VIOLATIONS OF LAW, REGULATION, AND CONTRAVENTIONS OF POLICY AND CORRECTION OF DEFICIENCIES

7. (a) Within 60 days from the effective date of this ORDER, the Bank shall eliminate and/or correct all IT violations of laws, regulations, and/or contraventions of IT statements of policy in the Report of Examination dated March 24, 2014 (Report) and shall adopt and implement appropriate procedures to ensure future compliance with all such applicable IT laws, regulations, and/or IT statements of policy.

(b) Within 90 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.

SHAREHOLDER DISCLOSURE

8. 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

9. Within 30 days from the end of the first quarter following the effective date of this ORDER, and within 30 days from the end of each quarter thereafter, the Bank shall furnish written progress reports to the Supervisory Authorities 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.

Effective June 9, 2010, the FDIC and the Department issued a CONSENT ORDER regarding the Bank that was amended effective October 9, 2013. That CONSENT ORDER remains in full force and effect.

The provisions of this ORDER shall not bar, stop, or otherwise prevent the FDIC 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 this 2nd day of February 2015.

Timothy D. Flono for

By: _____

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

The Alabama Superintendent of Banks, having duly approved the foregoing ORDER, and the Bank, through its Board, agree that the issuance of said ORDER by the Federal Deposit Insurance Corporation shall be binding as between the Bank and the Alabama Superintendent of Banks to the same degree and legal effect that such ORDER would be binding on the Bank if the Alabama Superintendent of Banks had issued a separate ORDER that included and incorporated all the provisions of the foregoing ORDER pursuant to the provisions of Section 5-2A-12 of the Code of Alabama.

Dated this 2nd day of February, 2015.

/s/

_____

John D. Harrison
Superintendent of Banks
Alabama State Banking Department