FEDERAL DEPOSIT INSURANCE CORPORATION
WASHINGTON, D.C.

In the Matter of	)	CONSENT ORDER
PEOPLESSOUTH BANK COLQUITT, GEORGIA	)	FDIC-16-0187b
(Insured State Nonmember Bank)	)	

The Federal Deposit Insurance Corporation ("FDIC") is the appropriate Federal banking agency for PeoplesSouth Bank, Colquitt, Georgia ("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 December 8, 2016, that is accepted by the FDIC and the Georgia Department of Banking and Finance ("Department"). The Department may issue an order pursuant to section 7-1-91 of the Official Code of Georgia Annotated, Georgia Code Ann. Section 7-1-91 (1985).

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 including weaknesses in the Bank's Information Technology ("IT") program or the Bank's compliance with the Bank Secrecy Act, subchapter II of Chapter 53 of Title 31 of the United States Code, and its implementing rules issued by the U.S. Department of Treasury, 31 C.F.R. Chapter X; the FDIC's Bank Secrecy Act compliance regulations, 12 C.F.R. § 326.8; and the FDIC's suspicious activity report ("SAR") regulations, 12 C.F.R. Part 353 ("Part 353")

(collectively, "the BSA"), to the issuance of this Consent Order ("ORDER") by the FDIC and the Department. Having determined that the requirements for issuance of an order under 12 U.S.C. § 1818(b) and Georgia Code Ann. Section 7-1-91 (1985) have been satisfied, the FDIC and the Department hereby order that:

BOARD SUPERVISION

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 policies and objectives and for the supervision of all of the Bank's activities, consistent with the role and expertise commonly expected for directors of banks of comparable size. This participation shall include meetings to be held no less frequently than monthly at which, at a minimum, the following areas shall be reviewed: audit reports; internal control reviews including management's responses; high-risk deposit accounts; non-bank financial institutions; domestic Automated Clearing House transactions ("ACH"); BSA risk assessment; BSA staffing; BSA training; BSA independent testing; BSA compliance; reports regarding information technology ("IT"); 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 ("Directors' Committee"), consisting of at least five members, to oversee the Bank's compliance with the ORDER. At least four of the members of the Directors' Committee shall be directors not employed in any capacity by the Bank other than as a director. The Directors' Committee shall review monthly reports detailing the Bank's actions with respect to compliance with this ORDER. The Directors' Committee shall present a report detailing the Bank's adherence to this ORDER to the Board at each regularly scheduled Board meeting. Such report shall be recorded in the appropriate minutes of the Board's meetings and shall be retained

in the Bank's records. Establishment of this committee does not in any way diminish the responsibility of the entire Board to ensure compliance with the provisions of this ORDER.

BSA COMPLIANCE PROGRAM

2. Within 60 days from the effective date of this ORDER, the Bank shall develop, adopt, and implement its written plan ("Compliance Plan") for administration of a BSA and anti-money laundering ("AML") compliance program reasonably designed to ensure and maintain compliance with the BSA. The Bank shall submit the Compliance Plan to the Regional Director of the FDIC's Atlanta Regional Office ("Regional Director") and the Department (collectively "Supervisory Authorities") for review and comment. The Compliance Plan shall be consistent with the guidance set forth in the *Federal Financial Institutions Examination Council's Bank Secrecy Act/Anti-Money Laundering Examination Manual* (http://www.ffiec.gov/bsa_aml_infobase/default.htm) ("BSA Manual"). The Compliance Plan shall be tailored to address the risk profile of the Bank identified in the Bank's BSA risk assessment required by paragraph 3 of this ORDER and shall address all deficiencies and recommendations in the Report of Examination dated June 6, 2016 ("Report"). Upon receipt of the Supervisory Authorities' comments, if any, the Board shall revise, review, and approve the Compliance Plan. After the Board has approved the Compliance Plan, the review and approval shall be recorded in the minutes of the Board.

RISK ASSESSMENT

3. (a) Within 30 days from the effective date of the ORDER, the Board shall review and revise as appropriate its written policies, procedures, and processes for a risk assessment of the Bank's operations ("Risk Assessment") consistent with the guidance for BSA/AML Risk Assessments set forth in the BSA Manual.

(b) Within 60 days from the effective date of the ORDER, the Bank shall conduct a Risk Assessment and thereafter shall conduct a Risk Assessment no less than annually. The Board shall review and approve the Risk Assessment and forward it to the Supervisory Authorities with the progress report required by this ORDER that is next due following the Board's approval. The Risk Assessment shall weigh all relevant factors, including identification and measurement of the specific risk characteristics of the Bank's products, services, customers, affiliates, and geographic locations, with analysis of the major risk categories including foreign nationals, non-resident aliens, ACH transactions, high-risk deposit accounts, and non-bank financial institutions. The Risk Assessment shall address all pertinent risk factors that affect the overall BSA/AML risk profile of the Bank and the deficiencies and recommendations contained in the Report, and ensure that risk ratings are accurate and well supported by qualitative and quantitative data.

INTERNAL CONTROLS

4. (a) Within 60 days from completion of the Risk Assessment conducted pursuant to Paragraph 3, the Bank shall develop a system of internal controls designed to ensure full compliance with the BSA ("BSA Internal Controls") taking into account its size and risk profile and addressing the deficiencies and recommendations contained in the Report.

(b) At a minimum, the BSA Internal Controls shall include policies, procedures, and processes addressing the following areas:

(i) Suspicious Activity Monitoring and Reporting: Taking into account its size and risk profile, the Bank shall develop, adopt, and implement policies, procedures, processes, and systems for monitoring, detecting, and reporting suspicious activity being conducted in all areas within or through the Bank. The Board needs to ensure that the resources deployed are commensurate with the Bank's transaction volume levels and customers with

remote deposit capture ("RDC") and privately-owned automatic teller machines ("ATM"). The methodology used to perform transaction monitoring needs to be comprehensive and utilize multiple time periods to ensure that potentially suspicious activities are being appropriate identified and reported as necessary. The Bank shall monitor all areas of the Bank for suspicious activity, including, but not limited to: cash transactions, international and domestic wire transfers, ACH, foreign nationals, non-resident aliens, high-risk deposit accounts, RDC, privately-owned ATMs, and non-bank financial institution accounts. The Bank shall cause the timely, accurate, and complete filing of SARs. The Bank shall require the appropriate level of documentation and support for any decision to file or not to file a SAR.

(ii) Customer Due Diligence: The Bank shall review and enhance its customer due diligence ("CDD") policies, procedures, and processes for new and existing customers ("CDD Program"):

(A) the CDD Program shall be consistent with guidance for CDD set forth in the BSA Manual;

(B) the CDD Program shall operate in conjunction with the Bank's Customer Identification Program ("CIP"); and

(C) At a minimum, the CDD Program shall include:

(1) a risk rating system to assess the Bank's customer base to ensure that the risk level of each customer is accurately identified based on the potential for money laundering or other illicit activity posed by the customer's activities. Each risk rating assessment shall take into account the purpose of the account, the customer's business or occupation, the actual or anticipated type and volume of account activity, types of products and services offered, and locations and markets served by the customer;

(2) policies and procedures with respect to high-risk accounts and customers, including a formal visitation program for all high-risk customers, periodic update of risk grades based on changes in risk factors, and a process for obtaining higher-level approvals for accounts and transactions where appropriate;

(3) an appropriate level of ongoing monitoring commensurate with the customer's risk level to ensure that the Bank can reasonably detect suspicious activity and accurately determine whether the customer requires enhanced due diligence ("EDD");

(4) procedures for obtaining a sufficient level of customer information at account opening and appropriate analysis of that information to assist and support the risk rating assigned;

(5) procedures for documenting and supporting the risk analysis conducted under the CDD process, including procedures for validating risk ratings assigned at account opening and resolving issues in the event insufficient or inaccurate information is obtained; and

(6) procedures reasonably designed to ensure the timely identification and accurate reporting of known or suspected criminal activity, as required by Part 353.

(iii) Enhanced Due Diligence: The Bank shall establish EDD policies, procedures, and processes to conduct EDD necessary for those categories of customers that the Bank has reason to believe pose a heightened risk of suspicious activity ("EDD Program"), including, but not limited to, high-risk accounts:

(A) the EDD Program shall be consistent with the guidance for EDD set forth in the BSA Manual;

(B) the EDD Program shall operate in conjunction with the Bank's CIP and CDD policies, procedures and processes; and

(C) At a minimum, the EDD Program shall include:

(1) procedures to determine the frequency of ongoing reviews based on customer risk level;

(2) procedures to determine the appropriate documentation necessary to conduct and support ongoing reviews and analyses in order to reasonably understand the customer's normal and expected transactions; and

(3) procedures reasonably designed to ensure the timely identification and accurate reporting to law enforcement and the Supervisory Authorities of known or suspected criminal activity against or involving the Bank, as required by Part 353.

(iv) Account Aggregation: Taking into account its size and risk profile, the Bank shall develop, adopt, and implement policies, procedures, processes, and systems, including automated monitoring systems, to provide for adequate systems for account aggregation to ensure sufficient data exists to determine if SARs and Currency Transaction Reports ("CTRs") should be filed;

(v) Account/Transaction Monitoring and Reporting: The policies, procedures, and processes that comprise the Bank's BSA Internal Controls shall operate in conjunction with each other and shall be consistent with the guidance for account/transaction monitoring and reporting set forth in the BSA Manual, including dissemination of the high-risk customer list to appropriate departments within the Bank.

(vi) Required Reporting: The Bank's BSA Internal Controls shall provide for periodic reports that address activity by risk code. The reports shall also include tracking data to ensure appropriate CIP information is obtained, site visitations are conducted, and monitoring

and SAR reporting systems procedures are being implemented in a timely manner. Such reports shall be provided to the Board prior to each Board meeting.

(c) The Bank shall adopt and implement the BSA Internal Controls. The BSA Internal Controls shall be submitted to the Supervisory Authorities for review and comment. Within 30 days of receipt of the Supervisory Authorities' comments and after incorporation and adoption of all comments, the Board shall approve the revised BSA Internal Controls, which approval shall be recorded in the minutes of the Board meeting.

BSA TRAINING

5. (a) The Bank shall ensure that all appropriate personnel can comply with the requirements of the BSA applicable to the individual's specific responsibilities to assure the Bank's compliance with the BSA.

(b) Within 60 days from the effective date of this ORDER, the Bank shall develop, adopt, and implement effective training programs designed for the Board, management, and staff and their specific compliance responsibilities on all relevant aspects of laws, regulations, and Bank policies, procedures and processes relating to the BSA ("Training Program"). The Training Program shall ensure that all appropriate personnel can comply with the requirements of the BSA on an ongoing basis, including as they relate to high-risk accounts, products, and services. The Training Program should incorporate specialized training for internal auditors to identify BSA/AML issues. The Training Program shall, at a minimum, include:

(i) An overview of the BSA for new staff along with specific training designed for their specific duties and responsibilities upon hiring;

(ii) Training on the Bank's BSA, AML, and Office of Foreign Assets Control ("OFAC") policies, Compliance Plan, procedures and processes along with new rules and

requirements as they arise for appropriate personnel designed to address their specific duties and responsibilities;

(iii) A requirement that the Bank fully document the training of each employee with respect to the BSA, AML, and OFAC policies, procedures, and processes; and

(iv) A requirement that training be conducted no less frequently than annually.

BSA OFFICER AND STAFF

6. (a) Within 60 days from the effective date of the ORDER, the Bank shall assess its BSA staffing needs to ensure adequate qualified personnel are in place at all times. The assessment should be performed by parties with appropriate skills and expertise necessary for assessing the knowledge, experience, and qualifications of staff within the BSA function at the Bank.

(b) Within 90 days from the effective date of the ORDER, the Bank shall develop and implement a written plan of action to develop or recruit personnel and hire additional or replacement personnel with the requisite ability, experience, and other qualifications necessary to ensure BSA compliance ("BSA Staffing Plan"). The BSA Staffing Plan shall include, at a minimum, consideration of the Bank's size and growth plans, geographical areas served, products and services offered, and changes in the BSA, AML, and OFAC practices, procedures, rules, and regulations.

(c) The Board shall review and approve the BSA Staffing Plan. Periodically thereafter, but no less often than annually, the Bank shall assess its BSA staffing needs to ensure adequate and appropriate BSA staffing resources are in place at all times.

(d) As part of the BSA Staffing Plan, the Board shall designate a qualified individual or individuals ("BSA Officer"), acceptable to the Supervisory Authorities, with delegated authority and adequate time, training, and appropriate resources to implement the Bank's BSA

Compliance Program. The BSA Officer's qualifications shall be commensurate with the complexity of the Bank's activities and the appointment of the BSA Officer shall conform to the guidance regarding BSA officers set forth in the BSA Manual. The BSA Officer shall report to the Board and shall provide reports as required directly to the Board.

INDEPENDENT TESTING

7. (a) Within 30 days from the effective date of the ORDER, the Bank shall contract with an external independent testing firm that specializes in the BSA, AML, and OFAC rules and regulations for a review. The scope of the testing to be performed shall be in writing and reviewed and approved by the Board. Testing procedures shall be consistent with the guidance for independent testing set forth in the BSA Manual.

(b) Within 90 days from the effective date of the ORDER, the written testing results shall be provided to the Board. The Board shall review and approve the testing results including any recommendations within 60 days of completion of the testing. The Bank shall adopt and implement any recommendations from the independent testing. Thereafter, the Bank shall have independent testing performed no less than annually.

BSA REPORTS

8. The Bank shall ensure that all reports required by BSA including CTRs, SARs, Reports of International Transportation of Currency or Monetary Instruments, Reports of Foreign Bank and Financial Accounts, and any other similar or related reports required by law or regulation are completed accurately and properly filed within required timeframes.

LOOK BACK REVIEW

9. (a) Within 30 days from the effective date of this ORDER, the Bank shall engage an independent qualified firm, acceptable to the Supervisory Authorities, to conduct a review of all high-risk accounts based on the Bank's Risk Assessment conducted pursuant to this ORDER and

all high-risk transaction activity for the period beginning November 3, 2014, through the effective date of this ORDER to determine whether SARs and CTRs should be filed ("Look Back Review").

(b) Within 60 days from the effective date of this ORDER, the Bank shall submit to the Supervisory Authorities a written plan ("Look Back Review Plan") for non-objection that sets forth:

(i) The scope of the Look Back Review, including the types of transactions to be reviewed;

(ii) The methodology for conducting the Look Back Review, including any sampling procedures to be followed;

(iii) The expertise and resources devoted to the Look Back Review;

(iv) The anticipated completion date of the Look Back Review; and

(v) A commitment that any interim reports, draft reports or work papers associated with the Look Back Review will be made available to the Supervisory Authorities upon request.

(c) Within 120 days of receipt of the Supervisory Authorities' non-objection to the Look Back Review Plan, the Look Back Review shall be completed and submitted to the Board. The Bank shall prepare and file any CTRs and SARs necessary based on the review.

(d) The review firm shall present its findings from the Look Back Review directly to the Board at a Board meeting and the presentation, conclusions, and discussion of the findings shall be reflected in the minutes for the meeting.

(e) Upon completion of the Look Back Review, the Bank shall submit a copy of the Look Back Review and copies of any additional SARs and CTRs filed to the Supervisory Authorities.

VIOLATIONS OF LAW, REGULATION, AND CONTRAVENTION OF POLICY

10. Within 60 days from the effective date of this ORDER, the Bank will eliminate and/or correct all violations of laws, regulations, and/or contraventions of statements of policy in the Report and shall adopt and implement appropriate procedures to ensure future compliance with all such applicable federal and state laws, regulations, and/or statements of policy.

INFORMATION TECHNOLOGY PLAN

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

(i) Development and implementation of the ongoing internal and external IT audit programs;

(ii) A written IT strategic plan required by Paragraph 13 of this ORDER that includes measurable goals for IT;

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

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

(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 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) A formal project management policy to support all IT projects and the purchase of equipment including project budgeting, testing, completion time frames, security, quality assurance guidelines and review processes, 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;

(x) The establishment of an on-going process-oriented approach to business continuity planning that includes a business impact analysis and disaster recovery plan and is revised in a timely manner based on problems noted during testing and changes in business operations.

(xi) All IT policies and procedures should sufficiently address all relevant areas detailed in the *FFIEC IT Handbooks* applicable to the Bank; and

(xii) A written plan to correct all IT deficiencies identified in the Report.

(b) The Board shall approve, adopt, and implement the IT Plan, and such approval shall be recorded in the minutes of the Board meeting.

INFORMATION SECURITY OFFICER AND STAFF

12. (a) Within 30 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.

(b) Within 60 days from the effective date of this ORDER, the Board shall appoint an Information Security Officer ("ISO") with the requisite skills, knowledge, and expertise, necessary to oversee the development, implementation, and maintenance of the IT Plan and other IT policies and procedures. 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 *FFIEC IT Booklet on Information Security*. The ISO shall report to the Board.

IT STRATEGIC PLAN

13. Within 90 days from the effective date of this ORDER, the Board shall develop its 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 factors detailed in the *FFIEC IT Booklet on Management* including resources needed for support and security of IT activities; strategies for mitigating risks; appropriate information security controls; appropriate segregation of duties; appropriate user access to the IT area; budgeting; periodic Board reporting; sufficient IT staffing; goals for the IT audit function; risk management controls supporting IT; and contingency planning for the replacement of IT functions and services should an unexpected interruption or loss of service occur. The IT Strategic Plan shall address all criticisms in the Report. The Board shall approve, adopt, and implement the IT Strategic Plan, and such approval shall be recorded in the minutes of the Board meeting.

PROGRESS REPORTS

14. 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.

DISCLOSURE TO SHAREHOLDERS

15. 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.

OTHER ACTIONS

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 by the Supervisory Authorities.

Issued Pursuant to Delegated Authority,

Dated: December 19th, 2016

By:

/s/

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

The Georgia Department of Banking and Finance having duly approved the foregoing ORDER, 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 Georgia Commissioner of Banking and Finance to the same degree and to the same legal effect that such ORDER would be binding if the Department had issued a separate ORDER that included and incorporated all of the provisions of the foregoing ORDER, pursuant to Official Code of Georgia Annotated § 7-1-91(1985).

Dated: December 12, 2016

By: ___/s/_____
Kevin B. Hagler
Commissioner
Department of Banking and Finance
State of Georgia