

FEDERAL DEPOSIT INSURANCE CORPORATION
WASHINGTON, D.C.

_____)	
In the Matter of)	CONSENT ORDER
BRIGHTON BANK)	
BRIGHTON, TENNESSEE)	FDIC-23-0069b
(Insured State Nonmember Bank))	
_____)	

The Federal Deposit Insurance Corporation (“FDIC”) is the appropriate Federal banking agency for BRIGHTON BANK, BRIGHTON, TENNESSEE (Bank), under Section 3(q) of the Federal Deposit Insurance Act (FDI 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 TO THE ISSUANCE OF A CONSENT ORDER” (“STIPULATION”), dated November 29, 2023, that is accepted by the FDIC. With the Stipulation, the Bank has consented, without admitting or denying any charges of violating the law relating to the Bank Secrecy Act, 31 U.S.C. §§ 5311 *et. seq.*, 12 U.S.C. § 1829b, and 12 U.S.C. §§ 1951-60 and the implementing regulations, 31 C.F.R. Chapter X, and 12 U.S.C. § 1818(s) and its implementing regulations, 12 C.F.R. § 353 and 12 C.F.R. § 326.8 (collectively referred to as the Bank Secrecy Act or BSA) and weaknesses in board and management oversight of the information technology function, to the issuance of this CONSENT ORDER (“ORDER”) by the FDIC pursuant to Section 8(b)(1) of the FDI Act.

Having determined that the requirements for issuance of an ORDER under Section 8(b) of the FDI Act, 12 U.S.C. § 1818(b) have been satisfied, the FDIC hereby orders that:

COMPLIANCE COMMITTEE

1. Within 30 days of the effective date of this ORDER, the Bank's Board shall establish a sub-committee of the Bank's Board charged with the responsibility of ensuring that the Bank complies with the provisions of this ORDER (Consent Order Compliance Committee). The Consent Order Compliance Committee shall report monthly to the entire Board, and a copy of the report and any discussions related to the report, or the ORDER shall be included in the minutes of the Bank's Board meeting. Nothing contained herein shall diminish the responsibility of the entire Board to ensure compliance with the provisions of this ORDER.

VIOLATIONS OF LAWS AND REGULATIONS

2. Within 90 days of the effective date of this ORDER, the Board shall eliminate and/or correct all violations of law, as more fully set forth in the Joint Report of Examination dated August 22, 2022 (ROE). In addition, the Bank shall take all necessary steps to ensure future compliance with all applicable laws and regulations.

ACTION PLAN

3. Within 45 days of the effective date of this ORDER, the Bank shall develop and implement a written action plan (Action Plan) that details the actions, including the relevant timelines, that the Board and management will take to correct the Bank's Anti-Money Laundering/Countering the Financing for Terrorism (AML/CFT) Program deficiencies and apparent violations cited in the ROE, and to comply with this ORDER. Such Plan and its implementation shall be acceptable to the Regional Director of the FDIC's Dallas Regional Office (Regional Director) as determined at subsequent examinations and/or visitations.

BOARD SUPERVISION

4. (a) Within 30 days after the effective date of this ORDER, the Board shall

increase its participation in the affairs of the Bank by assuming full responsibility for the supervision of the Bank's Information Technology (IT) function through the development and approval of the Bank's IT policies that reflect the Bank's current operating environment.

(b) The Bank shall ensure the Board, or a designated Board committee with sufficient time and expertise, actively monitors IT operations, including significant IT changes, and maintains formal minutes. The Board's participation in the Bank's affairs shall include, at a minimum, monthly meetings in which the IT program and associated tests of the program are reviewed. The Bank's Board minutes shall document the Board's reviews and approvals, including the names of any dissenting directors.

BOARD AND MANAGEMENT OVERSIGHT

5. (a) Within 120 days after the effective date of this ORDER, the Board shall have and retain qualified IT program management. At a minimum, such management shall include:

(1) An IT program manager(s) with the necessary training, experience, knowledge of bank systems and applications, and resources to manage the IT program and Information Security Program.

(2) Such persons shall be provided the necessary written authority to implement the provisions of this ORDER.

(b) The qualifications of IT management shall be assessed on the ability to:

(1) Comply with the requirements of this ORDER; and

(2) Comply with applicable laws and regulations.

(c) While this ORDER is in effect, the Board shall notify the Regional Director in writing of any changes in any of the Bank's Senior Executive Officers and the IT

program manager. For the purpose of this ORDER, “Senior Executive Officer” is defined as in Section 303.101(b) of the FDIC’s Rules and Regulations, 12 C.F.R. § 303.101(b).

(d) Within 120 days after the effective date of this ORDER, the Board shall implement effective monitoring procedures for on-going evaluation of security services performed by third parties, including managed security service providers. The Board shall assign independent responsibility for ongoing monitoring.

(e) Within 120 days of the effective date of this ORDER, the Board shall approve a comprehensive and detailed IT Strategic Plan that addresses the findings and recommendations noted in the ROE. The detailed IT Strategic Plan should be specific to the IT environment and focus on management's short-term and long-term plans, budget, and resource needs.

CYBERSECURITY PROGRAM

6. Within 90 days after the effective date of this ORDER, the Board shall address the deficiencies in the cybersecurity program by performing, or causing to be performed, a cybersecurity preparedness assessment, which identifies, measures, and reports cybersecurity-related risks in accordance with Information Security Standards; by evaluating the maturity of the cybersecurity program and identifying control gaps; and by remediating high-risk findings included in the 2022 third-party penetration test. The Board shall monitor the updated status of all baseline control gaps and remediate associated deficiencies in a timely manner.

AUDIT PROGRAM

7. (a) Within 90 days after the effective date of this ORDER, the Board shall designate and formally approve an audit committee that is responsible for on-going oversight of IT audit activities and require retention of formal minutes of committee discussions.

(b) Within 90 days after the effective date of this ORDER, the Board shall develop and implement a comprehensive IT Audit Program. The IT Audit Program shall provide comprehensive and continuous audit coverage, the scope of which shall be based on a comprehensive risk assessment. The IT Audit Program shall include an independent IT general controls audit, penetration test, and vulnerability assessment at least annually, or more frequently, if significant IT changes occur. The IT Audit Program must identify the scope, type, and frequency of various types of IT audits that will be performed.

(c) Within 90 days after the effective date of this ORDER, the Board shall enhance the audit tracking report to include all IT audit findings, such as reviews of internal controls, automated clearing house (ACH), wires, vulnerability assessments, and penetration tests, and regulatory exams including remediating all prior IT findings. Reports shall be presented to the Board for review with the review noted in the Bank's board minutes.

(d) Within 120 days after the effective date of this ORDER, the Board and Senior management shall address all prior IT audit and IT examination findings, since several are repeat findings.

SUPPORT AND DELIVERY

8. (a) Within 90 days after the effective date of this ORDER, the Board shall schedule and complete a comprehensive and independent review of user access rights, including privileged users, ensuring assigned access rights are based on business needs and are in alignment with job roles and responsibilities.

(b) Within 60 days from the effective date of this ORDER, the Board shall analyze, review, compare, and approve wire access rights, wire limits, and wire verification processes when personnel changes are made and ensure associated wire controls and wire

insurance is reasonable when compared to wire risks. The Board shall ensure wire systems are appropriately patched, maintained, and supported.

BSA OFFICER

9. (a) Within 60 days after the effective date of this ORDER and during the life of this ORDER, the Bank shall designate a qualified individual or individuals responsible for coordinating and monitoring day-to-day compliance with the BSA pursuant to Section 326.8 of the FDIC's Rules and Regulations, 12 C.F.R. § 326.8 (BSA Officer). The adequacy of the BSA Officer shall be reviewed by the Regional Director based on subsequent examinations and/or visitations of the Bank. At a minimum, the BSA Officer shall:

- (1) Have sufficient resources, time, and executive authority to monitor and ensure compliance with the BSA and its implementing rules and regulations;
- (2) Be responsible for determining the adequacy of Bank Secrecy Act/Anti-Money Laundering (BSA/AML) staffing and for supervising such staff in complying with the BSA and its implementing rules and regulations;
- (3) Report to the Bank's Audit Committee on a regular basis, not less than quarterly, with respect to any BSA/AML matters;
- (4) Be responsible for ensuring the proper filing of Currency Transaction Reports (CTRs), Report of International Transportation of Currency or Monetary Instruments, and Suspicious Activity Reports (SARs) relating to BSA; and
- (5) The BSA Officer shall provide monthly comprehensive written

reports to the Bank's Consent Order Compliance Committee regarding the Bank's adherence to the Action Plan and this ORDER.

(b) During the life of this ORDER, the Bank shall notify the Regional Director in writing PRIOR to appointing any new BSA Officer, or materially changing the responsibilities of the BSA Officer. Such proposed appointment, employment or change in responsibilities shall not become effective unless and until a written notice of non-objection has been received from the Regional Director. The Bank shall also notify the Regional Director in writing of any individual and/or management level committee to which the Bank approved BSA Officer reports, and shall ensure this individual and/or committee has the requisite BSA experience to help administer an effective BSA/AML Compliance Program.

BSA STAFFING

10. Within 90 days after the effective date of this ORDER, the Board shall analyze and assess the Bank's staffing needs in order to provide for an adequate number of qualified staff for the Bank's BSA Department. The BSA Department staff shall be evaluated to determine whether these individuals possess the knowledge, skills, abilities, experience, training, and other necessary qualifications required to perform present and anticipated duties, including adherence to the Bank's BSA/AML Compliance Program, the requirements of the BSA regulations, and the provisions of this ORDER. The adequacy of BSA staffing shall be reviewed by the Regional Director based on subsequent examinations and/or visitations of the Bank.

INTERNAL CONTROLS

11. Within 120 days from the effective date of this ORDER, the Bank shall develop and subsequently maintain a system of internal controls that provides, at a minimum;

- (a) Policies, procedures, and systems for identifying, evaluating, monitoring, investigating, and reporting suspicious activity in the Bank's products, accounts, customers, services, and geographic areas, including:
 - (1) Establishment of meaningful thresholds for identifying accounts and customers for further monitoring, review and analyses;
 - (2) Periodic test and monitoring of such thresholds for their appropriateness to the Bank's products, customers, accounts, services, and geographic areas;
 - (3) Review of existing systems to ensure adequate referral of information about potentially suspicious activity through appropriate levels of management, including a policy for determining action to be taken in the event of multiple filings of SARs on the same customer, or in the event a correspondent or other customer fails to provide due diligence information. Such procedures shall describe the circumstances under which an account should be closed and the processes and procedures to be followed in doing so;
- (b) Procedures and/or systems for each business area of the Bank to produce periodic reports designed to identify unusual or suspicious activity, to monitor and evaluate unusual or suspicious activity,

and to maintain accurate information needed to produce these reports. In addition, the periodic reports should cover a broad range of timeframes, including individual days, a number of days, and a number of months, as appropriate, and should segregate transactions that pose a greater than normal risk for non-compliance with the BSA;

- (c) Documentation of management's decisions to file or not to file an SAR;
- (d) Systems to ensure timely, accurate, and complete filing of required SARs and any other similar or related reports required by law;
- (e) Development and maintenance of policies and procedures with respect to wire transfer recordkeeping, including requirements for complete information on beneficiaries and senders, as required by 31 C.F.R. § 1010.410; and
- (f) Procedures to ensure customers and transactions are being compared to current Office of Foreign Assets Control (OFAC) listings.

INDEPENDENT TESTING

12. Within 90 days from the effective date of this ORDER, the Bank shall establish and maintain an independent testing program for compliance by the Bank with the BSA and its implementing rules and regulations to be conducted either by:

- (a) A qualified outside party with the requisite ability to perform such tests and analysis; or

- (b) Bank personnel independent of the BSA function with the knowledge to conduct this function.
- (c) Such tests shall be conducted on an annual basis. The independent tests shall, at a minimum:
 - (1) Test the Bank's internal procedures for monitoring compliance with the BSA and its implementing rules and regulations, including interviews of employees who handle cash transactions;
 - (2) Sample large currency transactions followed by a review of the CTR filings;
 - (3) Test the validity and reasonableness of the customer exemptions granted by the Bank;
 - (4) Test the Bank's recordkeeping system for compliance with the BSA and its implementing rules and regulations, including, but not limited to:
 - a. Tests to ensure all reportable transactions have been identified;
 - b. Tests to ensure Bank personnel are reviewing all applicable reports, including monitoring reports for structuring activities; and
 - c. Tests to ensure compliance with OFAC provisions.
 - (5) Test the Bank's Customer Identification Procedures (CIP);
 - (6) Test the adequacy of the Bank's Training program

- (7) Document the scope of the testing procedures performed and the findings of the tests. The results of each independent test, as well as any apparent exceptions noted during the tests, shall be presented to the Board. The Board shall record the steps taken to correct any exceptions noted and address any recommendations made during each independent test in the minutes of the Board meeting, or applicable committee meeting.

TRAINING

13. Within 120 days of the effective date of this ORDER, the Bank shall develop an effective training program for management and staff on all relevant aspects of laws, regulations, and Bank policies and procedures relating to the Bank's BSA/AML Compliance Program. The training shall also be required for all Board members. This training shall be conducted at least annually and ensure that all appropriate personnel are aware of, and can comply with, the requirements of BSA and its implementing rules and regulations, including currency and monetary instruments reporting requirements and the reporting requirements associated with SARs, as well as all applicable OFAC provisions. Management should maintain a sign-in sheet for all training provided that includes the date of the training, what the training covered, who attended the training, and who conducted the training.

PROGRESS REPORTS

14. Within 45 days after the end of the first calendar quarter following the effective date of this ORDER, and within 30 days after the end of each successive calendar quarter, the Bank shall furnish written progress reports to the Regional Director 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 the ORDER have been accomplished and the Regional Director have released the Bank in writing from making additional reports.

BINDING EFFECT

15. (a) The provisions of this ORDER shall not bar, estop, 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, as that term is defined in Section 3(u) of the FDI Act, 12 U.S.C. § 1813(u).

(b) 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.

(c) 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 FDIC.

Issued pursuant to delegated authority this 30th day of November, 2023.

/s/ _____
J. Mark Love
Deputy Regional Director
Dallas Regional Office
Division of Risk Management Supervision
Federal Deposit Insurance Corporation