#2023-002

UNITED STATES OF AMERICA
DEPARTMENT OF THE TREASURY
OFFICE OF THE COMPTROLLER OF THE CURRENCY

In the Matter of:	)	
	)	
	)	AA-NE-2023-03
Lake Shore Savings Bank	)	
Dunkirk, New York	)	
	)	
	)	
	)	

CONSENT ORDER

WHEREAS, the Office of the Comptroller of the Currency ("OCC") has supervisory authority over Lake Shore Savings Bank, Dunkirk, New York ("Bank");

WHEREAS, the OCC intends to initiate cease and desist proceedings against the Bank pursuant to 12 U.S.C. § 1818(b), through the issuance of a Notice of Charges, for noncompliance with the July 13, 2022 Formal Agreement ("Formal Agreement"), including for unsafe or unsound practice(s) relating to information technology security and controls and information technology risk governance and Board of Directors ("Board") and management oversight of corporate risk governance. The OCC also found deficiencies, unsafe or unsound practice(s), and violations of law, rule, or regulation, related to Bank Secrecy Act ("BSA")/Anti-Money Laundering ("AML") risk management under 12 C.F.R. § 21.21, including internal controls, BSA officer, customer identification program, customer due diligence, enhanced due diligence, and beneficial ownership; and unsafe or unsound practice(s), and violations of law, rule, or regulation related to suspicious activity monitoring and reporting under 12 C.F.R. § 163.180.

WHEREAS, in the interest of cooperation and to avoid additional costs associated with administrative and judicial proceedings with respect to the above matter, the Bank, by and through its duly elected and acting Board, consents to the issuance of this Consent Order ("Order"), by the OCC through the duly authorized representative of the Comptroller of the Currency ("Comptroller"); and

NOW, THEREFORE, pursuant to the authority vested in the OCC by Section 8(b) of the Federal Deposit Insurance Act, as amended, 12 U.S.C. § 1818(b), the OCC hereby orders that:

ARTICLE I
JURISDICTION

(1) The Bank is an "insured depository institution" as that term is defined in 12 U.S.C. § 1813(c)(2).

(2) The Bank is a Federal savings association within the meaning of 12 U.S.C. § 1813(q)(1)(C), and is chartered and examined by the OCC. *See* 12 U.S.C. §§ 1461 *et seq.*, 5412(b)(2)(B).

(3) The OCC is the "appropriate Federal banking agency" as that term is defined in 12 U.S.C. § 1813(q) and is therefore authorized to initiate and maintain this cease and desist action against the Bank pursuant to 12 U.S.C. § 1818(b).

ARTICLE II
COMPTROLLER'S FINDINGS

(1) The Comptroller finds, and the Bank neither admits nor denies, the following:

(a) the Bank is in substantial noncompliance with the requirements of the Articles of the Formal Agreement and has engaged in unsafe and unsound practices, and violations of law, rule, or regulation related to Compliance Committee, Board to Ensure Competent Management, Information Technology Governance Program; Information Security Program, and Automated Clearing House ("ACH") Risk Management Program; and

(b) the Bank has engaged in various unsafe and unsound practices and violations of law, rule, or regulation related to BSA/AML risk management under 12 C.F.R. § 21.21, including internal controls, BSA officer, customer identification program, customer due diligence, enhanced due diligence, and beneficial ownership; and the Bank has engaged in various unsafe or unsound practice(s), and violations of law, rule, or regulation related to suspicious activity monitoring and reporting under 12 C.F.R. § 163.180.

ARTICLE III
COMPLIANCE COMMITTEE

(1) The Board shall maintain a Compliance Committee of at least three (3) members of which a majority shall be directors who are not employees or officers of the Bank or any of its subsidiaries or affiliates. The Board shall confirm in writing to the Assistant Deputy Comptroller the names of the members of the Compliance Committee within ten (10) days of the effective date of this Order. In the event of a change of the membership, the Board shall submit in writing to the Assistant Deputy Comptroller within ten (10) days the name of any new or resigning committee member. The Compliance Committee shall monitor and oversee the Bank's

compliance with the provisions of this Order. The Compliance Committee shall meet at least monthly and maintain minutes of its meetings.

(2) By March 31, 2023, and thereafter within ten (10) days after the end of each calendar month, the Compliance Committee shall submit to the Board a written progress report setting forth in detail:

(a) a detailed and complete description of the corrective actions needed to achieve compliance with each Article of this Order;

(b) the specific corrective actions undertaken to comply with each Article of this Order; and

(c) the results and status of the corrective actions.

(3) Upon receiving each written progress report, the Board shall forward a copy of the report, with any additional comments by the Board, to the Assistant Deputy Comptroller within ten (10) days of the first Board meeting following the Board's receipt of such report.

ARTICLE IV
BOARD OVERSIGHT TO ENSURE COMPETENT MANAGEMENT

(1) Within thirty (30) days of the effective date of this Order, the Board shall develop, adopt, implement, and thereafter ensure the Bank's adherence to a program for corporate governance and Board oversight of the Bank's operation and structure. The Board shall submit a copy of this program to the Assistant Deputy Comptroller within ten (10) days of its adoption. At a minimum, the Board shall ensure that the program addresses the following:

(a) an independent third-party review of the Board's oversight and supervision of management to include:

(i) an assessment of individual director's and the Board's overall strengths and weaknesses and creation of a plan for a director education program to address identified weaknesses;

(ii) an assessment of whether Board members are receiving adequate information on Bank operations to enable them to fulfill their fiduciary responsibilities;

(iii) recommendations, as necessary, for the expansion of the scope, frequency, and sufficiency of information provided to the Board by management; and

(iv) identification of any deficiencies in current management's performance of their duties and development and implementation of a written program designed to ensure officers have the requisite skills and abilities necessary to supervise effectively and perform their duties on an ongoing basis;

Within thirty (30) days of the effective date of this Order, the Bank shall submit to the Assistant Deputy Comptroller for prior written determination of no supervisory objection, the name and qualifications of a proposed independent, third party consultant to conduct this review and provide a written report on the issues outlined in subsections (i) through (iv) above;

(b) processes and procedures to ensure the Board receives and reviews sufficient information from management, including scope, frequency, and content of the information, to enable the Board to oversee the Bank's operations in a safe and sound manner, make informed decisions, oversee the Bank's compliance with laws and regulations, oversee compliance with this Order, and fulfill their

fiduciary duties and other responsibilities under law; Refer to the OCC "Director's Handbook" (November 2020) and OCC Corporate and Risk Governance Booklet of the *Comptroller's Handbook* (July 2019);

(c) periodic audits to validate the integrity of the information provided to the board by management; and

(d) processes and procedures to ensure Board oversight and management accountability to address compliance with the terms of this Order.

(2) Within thirty (30) days of the effective date of this Order, the Board shall establish, and review at least annually, the objectives by which senior executive officers', as well as the Chief Technology Officer's, the Information Security Officer's, and the BSA Officer's, effectiveness will be measured. The Board shall perform and prepare an annual written performance appraisal for each Bank senior executive officer that evaluates performance according to the position's description and responsibilities, adherence to the Strategic Plan mandated in Article V below, objectives established by the Board, and the effectiveness of developing and successfully implementing action plans to address and remedy issues raised in this Order, Reports of Examination or audit reports. Upon completion, copies of each performance appraisal shall be submitted to the Assistant Deputy Comptroller.

(3) Within sixty (60) days of the effective date of this Order, and on an ongoing basis thereafter, the Board shall ensure that the Bank has competent management in place on a permanent and full-time basis, including but not limited to the Chief Executive Officer, Chief Operating Officer, Chief Technology Officer, Information Security Officer, and BSA Officer positions, vested with sufficient authority to fulfill the duties and responsibilities of the position, carry out the Board's policies, ensure the Bank's adherence to corporate

governance and decision-making processes, ensure compliance with this Order, applicable laws, rules and regulations, and manage the day-to-day operations of the Bank in a safe and sound manner within the scope of that position's responsibilities.

(4) For incumbent officers in the positions listed in paragraph (3) of this Article, the Board shall, within sixty (60) days of the effective date of this Order, assess each of these officer's experience, qualifications and performance compared to the position's description, duties and responsibilities, as well as their capabilities to perform present and anticipated duties and determine whether management changes will be made, including the need for additions to or deletions from current management.

(5) If the Board determines that an officer will continue in his or her position, but that the officer's depth of skills needs improvement, the Board shall within fifteen (15) days of such determination, develop and implement a written program, with specific time frames, to improve the officer's supervision and management of the Bank. At a minimum, the written program shall include:

(a) an education program designed to ensure that the officer has skills and abilities necessary to supervise effectively;

(b) a program to improve the effectiveness of the officer;

(c) objectives by which the officer's effectiveness will be measured; and

(d) a performance appraisal program and projected timeline for evaluating performance according to the position's description and responsibilities and for measuring performance against the Bank's goals and objectives.

Upon completion, a copy of the written program shall be submitted to the Assistant Deputy Comptroller.

(6) If any position specified in paragraph (2) or (3) of this Article becomes vacant, the Board shall, within ninety (90) days of such vacancy, identify and appoint a capable person to the vacant position, subject to the requirements of 12 C.F.R. § 5.51, who shall be vested with sufficient executive authority, time, and resources to ensure the Bank's compliance with this Order and the safe and sound operation of functions within the scope of that position's responsibility.

ARTICLE V
STRATEGIC PLAN

(1) Within sixty (60) days of the effective date of this Order, the Board shall submit to the Assistant Deputy Comptroller for review and prior written determination of no supervisory objection an acceptable a written strategic plan for the Bank, covering at least a three-year period ("Strategic Plan"). The Strategic Plan shall establish objectives for the Bank's overall risk profile, earnings performance, growth, balance sheet mix, off-balance sheet activities, liability structure, and capital and liquidity adequacy, together with strategies to achieve those objectives, and shall, at a minimum, include:

(a) a mission statement that forms the framework for the establishment of strategic goals and objectives;

(b) the strategic goals and objectives to be accomplished, including key financial indicators and risk tolerances;

(c) an assessment of the Bank's strengths, weaknesses, opportunities and threats that impact its strategic goals and objectives;

(d) an evaluation of the Bank's internal operations, staffing requirements, board and management information systems, policies, and procedures for their adequacy and contribution to the accomplishment of the strategic goals and objectives developed under paragraph (1)(b) of this Article;

(e) a management employment and succession plan designed to promote adequate staffing and continuity of capable management;

(f) a realistic and comprehensive budget that corresponds to the Strategic Plan's goals and objectives;

(g) a financial forecast to include projections for major balance sheet and income statement accounts and desired financial ratios over the period covered by the Strategic Plan;

(h) an identification and prioritization of initiatives and opportunities, including timeframes that comply with the requirements of this Order;

(i) a description of the Bank's target market(s) and competitive factors in its identified target market(s), and a description of controls systems to mitigate risks in the Bank's target market(s);

(j) an identification and assessment of the present and planned product lines (assets and liabilities) and the identification of appropriate risk management systems to identify, measure, monitor, and control risks within the product lines;

(k) concentration limits commensurate with the Bank's strategic goals and objectives and risk profile;

(l) assigned roles, responsibilities, and accountability for the strategic planning; and

(m) a description of systems and metrics designed to monitor the Bank's progress in meeting the Strategic Plan's goals and objectives.

(2) Within thirty (30) days following receipt of the Assistant Deputy Comptroller's written determination of no supervisory objection to the Strategic Plan or to any subsequent amendment to the Strategic Plan, the Board shall adopt and Bank management, subject to Board review and ongoing monitoring, shall immediately implement and thereafter ensure adherence to the Strategic Plan. The Board shall review the effectiveness of the Strategic Plan at least annually, no later than December 31 each year, and more frequently if necessary or if required by the OCC in writing, and amend the Strategic Plan as needed or directed by the OCC. Any amendment to the Strategic Plan must be submitted to the Assistant Deputy Comptroller for review and prior written determination of no supervisory objection.

(3) Until the Strategic Plan required under this Article has been submitted by the Bank for the Assistant Deputy Comptroller's review, has received a written determination of no supervisory objection from the Assistant Deputy Comptroller and has been adopted by the Board, the Bank shall not significantly deviate from the products, services, asset composition and size, funding sources, structure, operations, policies, procedures, and markets of the Bank that existed immediately before the effective date of this Order without first obtaining the Assistant Deputy Comptroller's prior written determination of no supervisory objection to such significant deviation.

(4) The Bank may not initiate any action that significantly deviates from a Strategic Plan (that has received written determination of no supervisory objection from the Assistant Deputy Comptroller and has been adopted by the Board) without a prior written determination of no supervisory objection from the Assistant Deputy Comptroller.

(5) Any request by the Bank for prior written determination of no supervisory objection to a significant deviation described in paragraphs (3) or (4) of this Article shall be submitted in writing to the Assistant Deputy Comptroller at least thirty (30) days in advance of the proposed significant deviation. Such written request by the Bank shall include an assessment of the effects of such proposed change on the Bank's condition and risk profile, including a profitability analysis and an evaluation of the adequacy of the Bank's organizational structure, staffing, management information systems, internal controls, and written policies and procedures to identify, measure, monitor, and control the risks associated with the proposed change.

(6) For the purposes of this Article, changes that may constitute a significant deviation include, but are not limited to, a change in the Bank's marketing strategies, products and services, marketing partners, underwriting practices and standards, credit administration, account management, collection strategies or operations, fee structure or pricing, accounting processes and practices, or funding strategy, any of which, alone or in the aggregate, may have a material effect on the Bank's operations or financial performance; or any other changes in personnel, operations, or external factors that may have a material effect on the Bank's operations or financial performance.

(7) At least monthly, a written evaluation of the Bank's performance against the Strategic Plan shall be prepared by Bank management and submitted to the Board. Within ten (10) days after submission of the evaluation, the Board shall review the evaluation and determine the corrective actions the Board will require Bank management to take to address any identified shortcomings. The Board's review of the evaluation and discussion of any required corrective actions to address any identified shortcomings shall be documented in the Board's meeting minutes. Upon completion of the Board's review, the Board shall submit to the Assistant Deputy

Comptroller a copy of the evaluation as well as a detailed description of the corrective actions the Board will require the Bank to take to address any identified shortcomings.

ARTICLE VI
INTERNAL AUDIT

(1) Within sixty (60) days of the effective date of this Order, the Bank shall submit to the Assistant Deputy Comptroller for review an acceptable, comprehensive, a written internal audit program that adequately assesses controls and operations to allow the Board and management to understand the sufficiency of the Bank's internal controls program ("Internal Audit Program").

(2) Management shall ensure the Internal Audit Program's compliance with the standards for internal audit systems set forth in Section II.B of the Interagency Guidelines Establishing Standards for Safety and Soundness, Appendix A to 12 C.F.R. Part 30. Refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook* for related safe and sound principles. The Internal Audit Program shall incorporate standards of safety and soundness that are commensurate with the Bank's size, complexity, scope of activities, and risk profile and shall, at a minimum:

(a) require the development of an internal audit policy and plan that is risk-based and provides adequate audit scope, coverage, issue tracking, and frequency for all areas of the Bank, including an information technology ("IT") audit, with

annual documented Board and Audit Committee approval of the internal audit plan and Board notification of any material variance from the plan;

(b) address the use of third-parties to complete any internal audit activities, including documented Board approval of selection and termination of third-parties; refer to OCC Bulletin 2013-29, "Third-Party Relationships" for related safe and sound principles;

(c) evaluate the reliability, adequacy, and effectiveness of the Bank's internal controls system, whether operated by the Bank or a third-party;

(d) evaluate whether the Bank's internal controls system results in prompt and accurate recording of transactions and proper safeguarding of assets;

(e) determine whether the Bank complies with laws and regulations and adheres to its established policies, procedures, and processes;

(f) determine whether management is taking appropriate and timely steps to address control deficiencies and audit report recommendations, that the progress of such steps is adequately validated, documented, and tracked, and that such progress is reported to the Audit Committee and the Board on at least a monthly basis;

(g) require all internal audit reports to be in writing and distributed directly to the Board, and not through any intervening party, and to be presented by the auditor to the Board in a timely manner after audit completion; and

(h) require audit work papers and documentation that provides a meaningful audit trail and validation for audit findings, conclusions, and recommendations.

(3) The Board shall provide effective oversight of the Internal Audit Program, including:

(a) verifying that management has adequately staffed the internal audit function, using internal resources and/or third-parties, with respect to both the number of auditors required and their knowledge, skills, and experience;

(b) verifying the internal audit function is independent and objective. The person responsible for implementing the Internal Audit Program shall functionally report directly to the Audit Committee, which shall direct his or her activities, set compensation, and evaluate performance;

(c) verifying management's actions to address material weaknesses in a timely manner and, where appropriate, directing management to take additional action; and

(d) verifying management satisfies all statutory, regulatory, and supervisory requirements.

(4) The internal audit staff shall have access to any records necessary for the proper conduct of its activities. The OCC shall have access to all reports and work papers of the internal audit staff and any third parties providing internal audit services.

(5) The Board shall adopt and Bank management, subject to Board review and ongoing monitoring, shall immediately implement and thereafter ensure adherence to the Internal Audit Program. The Board shall review the effectiveness of the Internal Audit Program at least annually, and more frequently if necessary or if required by the OCC in writing, and amend the Internal Audit Program as needed or directed by the OCC.

ARTICLE VII
INFORMATION TECHNOLOGY GOVERNANCE PROGRAM

(1) Within thirty (30) days of the effective date of this Order, the Bank shall submit to the Assistant Deputy Comptroller for review and prior written determination of no supervisory objection an acceptable, written program to effectively assess and manage the Bank's information technology IT activities ("IT Governance Program"). Refer to Federal Financial Institutions Examination Council ("FFIEC"), IT Handbook, for related safe and sound principles. Although the Bank may outsource some or all of its IT functions, outsourcing does not change the Board's responsibility to ensure effective IT controls.

(2) The IT Governance Program shall be commensurate with the level of risk and complexity of the Bank's IT activities and shall, at a minimum, address the following:

(a) an effective IT risk governance program that establishes the roles, responsibilities, and accountability of the Board of directors and management; refer to the "Management" booklet of the FFIEC IT Examination Handbook;

(b) an effective IT Audit that is risk based and provides adequate IT audit scope, coverage, and frequency and includes a plan for the selection, due diligence, evaluation, and ongoing monitoring and Board and Audit Committee oversight of IT audit activities performed by third parties;

(c) an IT planning process with the following elements: long-term goals and the allocation of IT resources to achieve them; alignment of the IT strategic plan with the enterprise-wide business plan; identification and

measurement of risk before changes or new investment in technology are made; an IT infrastructure to support current and planned business operations; integration of IT spending into the budgeting process; refer to the "Management" booklet of the FFIEC IT Examination Handbook;

(d) hiring and training practices governed by appropriate policies to maintain competent and trained staff to fulfill respective roles in the Bank's IT program, including in the Information Security Officer position; refer to the "Management" booklet of the FFIEC IT Examination Handbook;

(e) an effective IT risk management process that includes: identification and measurement of risks to information and technology assets, within the Bank or controlled by third-party providers; mitigation of risks to an acceptable residual risk level in conformance with the board's risk appetite; and monitoring risk levels with results reported to the board and senior management; refer to the "Management" booklet of the FFIEC IT Examination Handbook;

(f) an effective, written, system architecture program to identify, acquire, install, and maintain appropriate IT systems with project management standards, procedures, and controls commensurate with the characteristics and risks of the Bank's development, acquisition, and maintenance activities; refer to the "Development and Acquisition" booklet of the FFIEC IT Examination Handbook;

(g) an effective written program with standards and controls over data structure, usage, and storage; refer to the "Operations" and "Development and Acquisition" booklets of the FFIEC IT Examination Handbook;

(h) appropriate system security controls including documenting an inventory of information system assets including hardware, software, information and connections; classify the information system assets based on risk; implement user access and authentication controls based on the principle of least privilege, including proper segregation of duties; refer to the "Information Security" booklet of the FFIEC IT Examination Handbook;

(i) an effective incident identification and assessment process and effective written Incident Response Program; refer to OCC Bulletin 2005-13 "Response Programs for Unauthorized Access to Customer Information and Customer Notice - Final Guidance";

(j) a written change management program that addresses controls over the introduction of changes, in a controlled manner, into the IT environment; implements effective patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) and application software are appropriately updated; and use vulnerability scanners periodically to identify vulnerabilities in a timely manner; refer to the "Information Security" and "Operations" booklets of the FFIEC IT Examination Handbook;

(k) operational controls, procedures, standards, and processes, including, but not limited to, an environmental survey, network topologies and data

flows, environmental controls, physical and logical security, personnel controls, conversions, back-ups, disposal, imaging, problem management, and user support; refer to the "Operations" booklet of the FFIEC IT Examination Handbook;

(l) an updated written, Board-approved, enterprise-wide business continuity management and resiliency process ("Business Continuity and Recovery Plan") that includes a Business Impact Analysis that assesses and prioritizes potential threat and disruption scenarios, including cyber events, based upon their impact on operations and probability of occurrence; periodic enterprise-wide tests; independent assessment of the tests; and, updating the plan regularly as needed; refer to the "Business Continuity Planning" and "Information Security" booklets of the FFIEC IT Examination Handbook;

(m) an IT assurance and testing program that is risk-based, written, and well- documented; identifies and addresses the areas of greatest IT and information security risk exposure; promotes sound IT and information security controls; evaluates the adequacy of planning, oversight, operating processes, internal controls, and compliance efforts; includes self-assessments, independent penetration tests, vulnerability assessments and audits in the assurance testing program; and promptly detects, reports, and tracks significant risks and deficiencies and corrective actions; refer to the

"Audit" and "Information Security" booklets of the FFIEC IT Examination Handbook; and

(n) an effective IT third-party risk management program to enable the Bank to effectively assess and manage the risks of IT services provided by third parties. At a minimum the program shall:

(i) address how the Bank identifies and assesses the inherent risks of the products, services, and activities performed by third parties;

(ii) detail how the Bank selects, assesses, and oversees the third parties;

(iii) detail the Bank's plan for ensuring the third-party provider has the necessary resources, infrastructure, organizational capabilities, and technology security controls and safeguards in place to protect customer data; and

(iv) provides for ongoing periodic monitoring of the third-party relationship activities and performance.

(3) Within ten (10) days following receipt of the Assistant Deputy Comptroller's written determination of no supervisory objection to the IT Governance Program or to any subsequent amendment to the IT Governance Program, the Board shall adopt and Bank management, subject to Board review and ongoing monitoring, shall immediately implement and thereafter adhere to the IT Governance Program.

(4) The Board shall review the effectiveness of the IT Governance Program at least annually, no later than December 31, and more frequently if necessary or if required by the OCC in writing, and amend the IT Governance Program as needed or as directed by the

OCC. Any amendment to the IT Governance Program must be submitted to the Assistant Deputy Comptroller for review and prior written determination of no supervisory objection.

ARTICLE VIII
INFORMATION SECURITY PROGRAM

(1) Within thirty (30) days of the effective date of this Order, the Bank shall submit to the Assistant Deputy Comptroller for review and prior written determination of no supervisory objection an acceptable, written Information Security Program that includes administrative, technical, and physical safeguards to ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; ensure the proper disposal of customer information; and ensure the overall safety and soundness of the Bank. Refer to the "Information Security" booklet of the FFIEC IT Examination Handbook for guidance.

(2) The Information Security Program shall comply with 12 C.F.R. Part 30, Appendix B, and shall, at a minimum, address the following:

(a) the Board's approval, or the approval of an appropriate Board committee, of the Information Security Program;

(b) a risk assessment that identifies reasonably foreseeable threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems; that assesses the likelihood and potential damage of these threats; that assesses the sufficiency

of policies, procedures, customer information systems, and other arrangements in place to control risks; and, that aligns with the Bank's enterprise-wide risk management program;

(c) measures to control identified risks, commensurate with the sensitivity of the information and the complexity and scope of the Bank's activities, including measures to address data loss prevention;

(d) dedicated Information Security Officer with sufficient authority to oversee and implement the Information Security Program;

(e) regular testing of key controls, systems, and procedures and independent testing or reviews of testing; including incident response testing and training;

(f) appropriate measures for the proper disposal of customer information and customer information systems; including measures to address data loss prevention;

(g) a process to monitor, evaluate and adjust, as appropriate, the program in response to changes in technology, the sensitivity of customer information, internal or external threats, changing business arrangements, changing outsourcing arrangements, and changing systems; and the annual receipt by the Board, or an appropriate committee thereof, of a report that describes the overall status of the Information Security Program and the Bank's compliance with 12 C.F.R. Part 30, Appendix B; and

(h) the annual receipt by the Board or appropriate committee thereof of a report that describes the overall status of the Information Security Program and the Bank's compliance with 12 C.F.R. Part 30, Appendix B.

(3) Within ten (10) days following receipt of the Assistant Deputy Comptroller's written determination of no supervisory objection to the Information Security Program or to any subsequent amendment to the Information Security Program, the Board shall adopt and Bank management, subject to Board review and ongoing monitoring, shall immediately implement and thereafter adhere to the Information Security Program.

(4) The Board shall review the effectiveness of the Information Security Program at least annually, and more frequently if necessary or if required by the OCC in writing, and amend the Information Security Program as needed or as directed by the OCC. Any amendment to the Information Security Program must be submitted to the Assistant Deputy Comptroller for review and prior written determination of no supervisory objection.

ARTICLE IX
ACH RISK MANAGEMENT PROGRAM

(1) The Board shall immediately adopt and implement the written ACH Risk Management Program ("ACH Program") previously given no supervisory objection by the Assistant Deputy Comptroller.

(2) The ACH Program shall at all times address, at a minimum:

(a) implementation of Board approved written risk-based policies, procedures, and processes for effective risk management of ACH activities appropriate for the size and complexity of the Bank, to include policies and

procedures relating to credit risk management, control requirements for ACH customers, and audit of ACH activities; and

(b) adequate staffing and defined resources at the Bank dedicated to the review and audit of ACH transactions to ensure ongoing compliance with ACH policies and procedures.

(3) The Board shall review the effectiveness of the ACH Program at least annually, and more frequently if necessary or if required by the OCC in writing, and amend the ACH Program as needed or directed by the OCC.

ARTICLE X
BSA OFFICER

(1) Within thirty (30) days of the effective date of this Order, the Bank shall analyze the current BSA/AML risk profile and strategic direction to determine the skills, experience, and expertise required of the Bank's BSA Officer. Based on this analysis, the Board shall develop a comprehensive job description detailing all the requirements and responsibilities of the BSA Officer role.

(2) Within ninety (90) days of the effective date of this Order, the Board shall ensure that the Bank's BSA Department maintains sufficient personnel with requisite expertise, training, skills, and authority. The Board shall ensure that the Bank has a permanent, qualified, and experienced BSA Officer who shall be vested with sufficient executive authority, time, and resources to fulfill the duties and responsibilities of the position and ensure the safe and sound operation of the Bank. The Board shall ensure that the responsibilities of the BSA Officer shall

be limited to overseeing and administering the development and implementation of an effective compliance program under the Bank Secrecy Act.

(3) In the event that the BSA Officer position is vacated, the Board shall, within sixty (60) days of such vacancy, appoint a capable person to the vacant position who shall be vested with sufficient executive authority, time, and resources to ensure the Bank's compliance with this Order and the safe and sound operation of functions within the scope of that position's responsibility.

(4) Prior to the permanent appointment of a BSA Officer under Paragraph (4) of this Article, the Board shall submit the name, resume, and such other information as the Assistant Deputy Comptroller may request, of a qualified individual or individuals to be responsible for coordinating and monitoring day-to-day compliance with the BSA for review and non-objection by the Assistant Deputy Comptroller. The Assistant Deputy Comptroller shall have the power to disapprove the appointment of the proposed new BSA Officer. The requirement to submit information and the prior disapproval provisions of this Paragraph (5) are based on the authority of 12 U.S.C. § 1818(b)(6)(E) and do not require the Assistant Deputy Comptroller to complete her review and act on any such information within ninety (90) days. The lack of disapproval of such individual shall not constitute an approval or endorsement of the proposed BSA Officer.

ARTICLE XI
BSA/AML INTERNAL CONTROLS

(1) Within sixty (60) days of the effective date of this Order, the Bank shall develop, adopt, implement, ensure that the BSA Officer and any supporting staff receive training, and thereafter ensure the Bank's adherence to a written system of internal controls reasonably

designed to provide for ongoing compliance with BSA regulatory requirements including appropriate suspicious activity monitoring and reporting. The Bank's system of internal controls must include, at a minimum:

(a) effective management information systems, commensurate with the Bank's size and risk profile, that provide timely and accurate periodic reporting to senior management and the Board of the status of the Bank's BSA/AML program, including, but not limited to, trends in suspicious activity reports ("SAR" or "SARs") and other filings, alert and investigation volumes, and compliance with the BSA and this Order;

(b) effective independent, risk-based quality assurance and quality control methodologies and processes, which shall include but not be limited to assessment of suspicious activity alerts and investigations, SAR filings, and periodic review of high-risk customers, with a focus on decision quality. The quality assurance and quality control processes shall review work performed by Bank personnel and third parties performing Bank BSA/AML functions;

(c) detailed, accurate documentation of personnel roles and responsibilities; and

(d) an effective issue tracking and reporting system to record findings made about the BSA/AML program by the Bank, the OCC, auditors, or third parties, and to make appropriate reporting to Bank management regarding the status of issue remediation. In all instances, the system shall make clear:

(i) what remediation is required to address the finding(s);

(ii) the due date for the remediation to be completed;

(iii) the specific reason(s) for any delay in meeting the remediation date; and

(iv) the person(s) within the Bank who are specifically responsible for ensuring that the remediation is timely completed and appropriately addresses the finding(s) made about the BSA/AML program.

ARTICLE XII
SUSPICIOUS ACTIVITY MONITORING AND REPORTING

(1) Within ninety (90) days of the effective date of this Order, the Board shall ensure that Bank management develops, implements, and thereafter maintains adherence to an enhanced written risk-based program of internal controls and processes to ensure compliance with the requirements to file SARs as set forth in 12 C.F.R. § 163.180. At a minimum, this written program shall:

(a) establish procedures for identifying, monitoring, and reporting suspicious activity, known or suspected violations of Federal law, violations of the BSA, or suspicious transactions related to money laundering activity across all lines of business, including suspicious activity relating to the opening of new accounts, the monitoring of current accounts, and the transfer of funds through the Bank, consistent with the Suspicious Activity Reporting section of the FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual;

(b) establish and apply appropriate thresholds and filters for the automated suspicious activity monitoring system ("SAM" or "SAMS") for monitoring all

types of transactions, accounts, customers, products, services, and geographic areas that include, at a minimum:

(i) meaningful thresholds and alert scenarios for filtering accounts and customers for further monitoring, review, and analyses;

(ii) maintenance of documentation supporting the Bank's methodology for establishing and altering threshold filters;

(iii) written documentation supporting the disposition of the suspicious activity alerts; and

(iv) periodic independent validation of thresholds and filters for their appropriateness to the Bank's customer base, products, services, and geographic area;

(c) establish procedures and processes and written documentation to support any decision not to file a SAR, which must include the alert type, nature of the transaction, nature of the customer, and any other information considered when making the decision to not file a SAR;

(d) establish procedures and processes and written documentation of any SAR escalated for additional investigation;

(e) provide for meaningful, accurate, and timely reporting to the Board and management of suspicious activity investigations and SAR filings; and

(f) ensure the Bank files SARs within he time frames specified in the applicable rules, regulations, and regulatory guidance, and files follow-up SARs every ninety (90) days in cases where suspicious activity is ongoing.

(2) The Board shall ensure that the Bank has processes, personnel, and control systems to implement and adhere to the program developed pursuant to this Article.

(3) The Board shall ensure that the BSA Officer and any supporting staff receive training on how to clear alerts, perform investigations, support No-SAR decisions and write SAR narratives consistent with FinCEN SAR filing guidance.

ARTICLE XIII
SUSPICIOUS ACTIVITY REVIEW LOOKBACK

(1) Within thirty (30) days of the effective date of this Order, the Bank shall submit to the Assistant Deputy Comptroller for prior written determination of no supervisory objection, the name and qualifications of a proposed independent, third-party consultant ("Look-Back Consultant") to conduct a review and provide a written report on the Bank's suspicious activity monitoring ("SAR Look-Back"). The Bank shall submit information regarding the Bank's due diligence, including the proposed independent consultant's qualifications and terms of engagement, in accordance with the requirements of OCC Bulletin 2013-33. Within thirty (30) days of the effective date of this Order, the Bank also shall submit, for a prior written determination of no supervisory objection, a proposed scope and timeline for completion of the engagement that addresses the requirements of paragraph (2) of this Article and includes a list of the customers, accounts, and alerts selected, and the methodologies, factors, and other considerations used to select the customers, account, and alerts.

(2) The scope of the SAR Look-Back shall include the Bank's medium risk or high risk activity for the period April 1, 2022 through September 30, 2022, and shall be risk-based, as

determined by annual volume, geography and product risk, and other factors. The scope of the SAR Look-Back also shall include account activity, for the same period for specific accounts:

(a) owned by high-risk customers; or

(b) that generated internal alerts for which the Bank determined it would not file a SAR.

(3) Within thirty (30) days of completion of the SAR Look-Back, the Look-Back Consultant shall provide the Board with a written report that contains a list of any SARs that the Look-Back Consultant recommends that the Bank should file, existing SARs that the Bank should modify to comply with the requirements of 12 C.F.R. § 163.180, a list of accounts that represent higher BSA/AML risk, and a conclusion about the effectiveness of the Bank's suspicious activity monitoring. This SAR Look-Back report also should describe:

(a) the methodologies and tools used in conducting the review;

(b) the process for investigating customers and customer activities;

(c) the number and types of customers and accounts reviewed;

(d) the number of customers and accounts requiring additional investigation;

(e) the number of customers the Look-Back Consultant recommended to the Bank that warranted SAR filings or modifications to existing SAR filings; and

(f) the number of customers where the Bank determined not to file a SAR.

When providing the written report to the Board, the Look-Back Consultant shall, at the same time, directly provide a copy of the written report of the findings and recommendations from the SAR Look-Back to the Assistant Deputy Comptroller. The supporting materials and work papers associated with the SAR Look-Back shall be made available to the OCC upon request.

(4) Based upon the results of the SAR Look-Back, the OCC, at its sole discretion may expand the scope of the SAR Look-Back period.

ARTICLE XIV
CUSTOMER INFORMATION PROGRAM, BENEFICIAL OWNERSHIP, CUSTOMER DUE DILIGENCE, and ENHANCED DUE DILIGENCE

(1) Within sixty (60) days of the effective date of this Order, the Bank shall revise, develop, adopt, implement, and thereafter ensure the Bank's adherence to expanded account opening policies and procedures for all accounts that pose greater than normal risk for compliance with the BSA. At a minimum, the policies and procedures shall include:

(a) appropriate risk-based policies and procedures, pursuant to 12 C.F.R. § 21.21(c)(2) and 31 C.F.R. § 1010.220, that enable the Bank to form a reasonable belief that it knows the true identity of its customers ("Customer Identification Program" or "CIP"); the Bank shall ensure CIP information on current and new customers is accurate and shall develop and implement a written plan to correct any inaccuracies in CIP information;

(b) appropriate risk-based policies and procedures, pursuant to 31 C.F.R. § 1010.230, that are reasonably designed to identify and verify beneficial owners of legal entity customers ("Beneficial Ownership" or "BO") ; the Bank shall ensure BO information on current and new customers is accurate and shall develop and implement a written plan to correct any inaccuracies;

(c) appropriate risk-based customer due diligence policies and procedures for conducting ongoing customer due diligence ("CDD") for all customers, pursuant to 31 C.F.R. § 1020.210(a)(2)(v), and particularly for high-risk customers that

present a higher risk for money laundering and terrorist financing ("Enhanced Due Diligence" or "EDD"); the Bank shall ensure sufficient CDD and EDD information is collected on all new and existing accounts to identify anticipated account activity that must be compared to actual activity to facilitate suspicious activity identification and shall develop and implement a written plan to correct any inaccuracies.

(2) Within ninety (90) days of the effective date of this Order, the BSA Officer shall complete a review of all high-risk customer accounts and account relationships to ensure CIP, BO, CDD, and EDD information for customer accounts is accurate and shall develop a formalized plan to correct all inaccuracies.

(3) Within ninety (90) days of the effective date of this Order and annually thereafter, the Board shall ensure that relevant BSA staff receive CIP, CDD, EDD, and BO documentation review training in accordance with the revised policies and procedures outlined in this Article.

(4) The Board shall ensure that the Bank has processes, personnel, and control systems to implement and adhere to the program developed pursuant to this Article.

ARTICLE XV
BSA/AML MODEL RISK MANAGEMENT

(1) Within sixty (60) days of the effective date of this Order, the Bank shall develop, adopt, implement, and thereafter ensure the Bank's adherence to procedures for periodically reviewing, testing, and updating the Bank's BSA/AML model risk assessments to cover risks associated with current, or subsequently proposed, Bank products, services, customers, entities, and geographies served, and including the dollar volume, number, and geographic markets

associated with Bank products, services, customers and transactions. The Bank's procedures must include, at a minimum:

(a) procedures to ensure the application of appropriate thresholds in the Bank's automated monitoring systems to filter accounts and customers for further monitoring, review, and analysis, including:

(i) an analysis of the existing filtering thresholds established by the Bank;

(ii) periodic review, testing, and monitoring of thresholds for their appropriateness to the Bank's customer base, products, services, and geographic areas;

(iii) requirements that any changes to filtering thresholds are approved at the senior management level and periodically reported to the Board;

(iv) requirements that documentation of any changes to the filtering thresholds is maintained and available to auditors and OCC examiners.

(2) Within ninety (90) days of the effective date of this Order, the Bank shall develop, adopt, implement, and thereafter ensure the Bank's adherence to requirements for the periodic independent validation of the Bank's BSA/AML SAMS to ensure the system is detecting potentially suspicious activity. The Bank's independent validation system must include, at a minimum:

(a) requirements for periodic independent validation of the models and filtering thresholds used for the BSA/AML monitoring systems in order to ensure that all accounts and transactions are captured, and the systems are adequate to detect potentially suspicious or sanctioned activity; and

(b) engaging a qualified, independent third-party to perform the periodic validations of the Bank's BSA/AML SAM system to ensure that the system is detecting potentially suspicious activity. The periodic validations must:

(i) assess the effectiveness of current parameters, algorithms and alert generation relative to the Bank's risk profile;

(ii) review the effectiveness of management's use of the model risk management;

(iii) ensure the independent third-party validations are reviewed by the Board; and

(iv) require management document the recommended changes that are implemented and support why any recommended changes are not implemented.

ARTICLE XVI
GENERAL BOARD RESPONSIBILITIES

(1) The Board shall ensure that the Bank has timely adopted and implemented all corrective actions required by this Order, and shall verify that the Bank adheres to the corrective actions and they are effective in addressing the Bank's deficiencies that resulted in this Order.

(2) In each instance in which this Order imposes responsibilities upon the Board, it is intended to mean that the Board shall:

(a) authorize, direct, and adopt corrective actions on behalf of the Bank as may be necessary to perform the obligations and undertakings imposed on the Board by this Order;

(b) ensure the Bank has sufficient processes, management, personnel, control systems, and corporate and risk governance to implement and adhere to all provisions of this Order;

(c) require that Bank management and personnel have sufficient training and authority to execute their duties and responsibilities pertaining to or resulting from this Order;

(d) hold Bank management and personnel accountable for executing their duties and responsibilities pertaining to or resulting from this Order;

(e) require appropriate, adequate, and timely reporting to the Board by Bank management of corrective actions directed by the Board to be taken under the terms of this Order; and

(f) address any noncompliance with corrective actions in a timely and appropriate manner.

ARTICLE XVII
WAIVERS

(1) The Bank, by executing and consenting to this Order, waives:

(a) any and all rights to the issuance of a Notice of Charges pursuant to 12 U.S.C. § 1818;

(b) any and all procedural rights available in connection with the issuance of this Order;

(c) any and all rights to a hearing and a final agency decision pursuant to 12 U.S.C. § 1818 and 12 C.F.R. Part 109;

(d) any and all rights to seek any type of administrative or judicial review of this Order;

(e) any and all claims for fees, costs, or expenses against the OCC, or any of its officers, employees, or agents related in any way to this enforcement matter or this Order, whether arising under common law or under the terms of any statute, including, but not limited to, the Equal Access to Justice Act, 5 U.S.C. § 504 and 28 U.S.C. § 2412;

(f) any and all rights to assert these proceedings, the consent to and/or the issuance of this Order, as the basis for a claim of double jeopardy in any pending or future proceedings brought by the United States Department of Justice or any other governmental entity; and

(g) any and all rights to challenge or contest the validity of this Order.

ARTICLE XVIII
OTHER PROVISIONS

(1) As a result of this Order, pursuant to 12 C.F.R. § 5.51(c)(7)(ii), the Bank is in "troubled condition," and is not an "eligible bank/savings association" for purposes of 12 C.F.R. § 5.3, unless otherwise informed in writing by the OCC.

(2) The Bank is subject to the restrictions in 12 C.F.R. § 5.51 requiring prior notice to the OCC of changes in directors and senior executive officers or the limitations on golden parachute payments set forth in 12 C.F.R. Part 359.

(3) This Order supersedes all prior OCC communications issued pursuant to 12 C.F.R. §§ 5.3, and 5.51(c)(7)(ii)).

ARTICLE XIX
CLOSING

(1) This Order is a settlement of the cease and desist proceedings against the Bank contemplated by the OCC, based on the unsafe or unsound practices, noncompliance with the Formal Agreement, and/or violations of law described in the Comptroller's Findings set forth in Article II of this Order. The OCC releases and discharges the Bank from all potential liability for a cease and desist order that has been or might have been asserted by the OCC based on the practices and/or violations described in Article II of this Order, to the extent known to the OCC as of the effective date of this Order. Nothing in this Order, however, shall prevent the OCC from:

(a) instituting enforcement actions other than a cease and desist order against the Bank based on the Comptroller's Findings set forth in Article II of this Order;

(b) instituting enforcement actions against the Bank based on any other findings;

(c) instituting enforcement actions against institution-affiliated parties (as defined by 12 U.S.C. § 1813(u)) based on the Comptroller's Findings set forth in Article II of this Order, or any other findings; or

(d) utilizing the Comptroller's Findings set forth in Article II of this Order in future enforcement actions against the Bank or its institution-affiliated parties to establish a pattern or the continuation of a pattern.

(2) Nothing in this Order is a release, discharge, compromise, settlement, dismissal, or resolution of any actions, or in any way affects any actions that may be or have been brought

by any other representative of the United States or an agency thereof, including, without limitation, the United States Department of Justice.

(3) This Order is:

(a) a "cease-and-desist order issued upon consent" within the meaning of 12 U.S.C. § 1818(b);

(b) a "cease-and-desist order which has become final" within the meaning of 12 U.S.C. § 1818(e);

(c) an "order issued with the consent of the depository institution" within the meaning of 12 U.S.C. § 1818(h)(2);

(d) an "effective and outstanding . . . order" within the meaning of 12 U.S.C. § 1818(i)(1); and

(e) a "final order" within the meaning of 12 U.S.C. § 1818(i)(2) and (u).

(4) This Order is effective upon its issuance by the OCC, through the Comptroller's duly authorized representative. Except as otherwise expressly provided herein, all references to "days" in this Order shall mean calendar days and the computation of any period of time imposed by this Order shall not include the date of the act or event that commences the period of time.

(5) The provisions of this Order shall remain effective except to the extent that, and until such time as, such provisions are amended, suspended, waived, or terminated in writing by the OCC, through the Comptroller's duly authorized representative. If the Bank seeks an extension, amendment, suspension, waiver, or termination of any provision of this Order, the Board or a Board-designee shall submit a written request to the signer's title asking for the desired relief. Any request submitted pursuant to this paragraph shall include a statement setting

forth in detail the circumstances that warrant the desired relief or prevent the Bank from complying with the relevant provision(s) of the Order, and shall be accompanied by relevant supporting documentation. The OCC's decision concerning a request submitted pursuant to this paragraph, which will be communicated to the Board in writing, is final and not subject to further review.

(6) The Bank will not be deemed to be in compliance with this Order until it has adopted, implemented, and adhered to all of the corrective actions set forth in each Article of this Order; the corrective actions are effective in addressing the Bank's deficiencies; and the OCC has verified and validated the corrective actions. An assessment of the effectiveness of the corrective actions requires sufficient passage of time for the Bank to demonstrate the sustained effectiveness of the corrective actions.

(7) This Order is not a contract binding on the United States, the United States Treasury Department, the OCC, or any officer, employee, or agent of the OCC and neither the Bank nor the OCC intends this Order to be a contract.

(8) Each citation, issuance, or guidance referenced in this Order includes any subsequent citation, issuance, or guidance that replaces, supersedes, amends, or revises the referenced cited citation, issuance, or guidance.

(9) This Order applies to the Bank and all its subsidiaries.

(10) No separate promise or inducement of any kind has been made by the OCC, or by its officers, employees, or agents, to cause or induce the Bank to consent to the issuance of this Order.

(11) All reports, plans, or programs submitted to the OCC pursuant to this Order shall be forwarded through the OCC's secure portal with an e-mail notification to the Assistant Deputy Comptroller.

(12) The terms of this Order, including this paragraph, are not subject to amendment or modification by any extraneous expression, prior agreements, or prior arrangements between the parties, whether oral or written.

IN TESTIMONY WHEREOF, the undersigned, authorized by the Comptroller as his duly authorized representative, has hereunto set his signature on behalf of the Comptroller.

/s/ Digitally Signed, Dated: 2023.02.09
James G. Bost
Assistant Deputy Comptroller
Office of the Comptroller of the Currency

_____
Date

IN TESTIMONY WHEREOF, the undersigned, as the duly elected and acting Board of Directors of Lake Shore Savings Bank have hereunto set their signatures on behalf of the Bank.

/s/	2/9/2023
Tracy S. Bennett	Date
/s/	2/9/2023
Sharon Brautigam	Date
/s/	2/9/2023
Michelle DeBergalis	Date
/s/	2/9/2023
John P. McGrath	Date
/s/	DocuSigned
Jack Mehltretter	Date
/s/	DocuSigned
Ronald Passafaro	Date
/s/	2/9/2023
Daniel P. Reininga	Date
/s/	2/9/23
Kevin M. Sanvidge	Date