

AGREEMENT BY AND BETWEEN  
Blue Ridge Bank, National Association  
Martinsville, Virginia  
and  
The Office of the Comptroller of the Currency

AA-NE-2022-43

Blue Ridge Bank, National Association, Martinsville, Virginia (“Bank”) and the Office of the Comptroller of the Currency (“OCC”) wish to assure the safety and soundness of the Bank and its compliance with laws and regulations.

The Comptroller of the Currency (“Comptroller”) has found unsafe or unsound practice(s), including those relating to third-party risk management, Bank Secrecy Act (“BSA”) /Anti Money Laundering (“AML”) risk management, suspicious activity reporting, and information technology control and risk governance.

Therefore, the OCC, through the duly authorized representative of the Comptroller, and the Bank, through its duly elected and acting Board of Directors (“Board”), hereby agree that the Bank shall operate at all times in compliance with the following:

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 national banking association within the meaning of 12 U.S.C. § 1813(q)(1)(A), and is chartered and examined by the OCC. *See* 12 U.S.C. § 1 *et seq.*

(3) The OCC is the “appropriate Federal banking agency” as that term is defined in 12 U.S.C. § 1813(q).

## ARTICLE II

### COMPLIANCE COMMITTEE

(1) Within ten (10) days of the date of this Agreement, the Board shall appoint 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 submit in writing to the Assistant Deputy Comptroller the names of the members of the Compliance Committee within ten (10) days of their appointment. 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 Agreement. The Compliance Committee shall meet at least quarterly and maintain minutes of its meetings.

(2) By December 31, 2022, and thereafter within thirty (30) days after the end of each quarter, the Compliance Committee shall submit to the Board a written progress report setting forth in detail:

- (a) a description of the corrective actions needed to achieve compliance with each Article of this Agreement, timelines to complete the corrective actions, as well as the person(s) responsible for completing the corrective actions;
- (b) the specific corrective actions undertaken to comply with each Article of this Agreement; 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 III

#### THIRD-PARTY RISK MANAGEMENT

(1) Within sixty (60) days of the date of this Agreement, the Board shall adopt and Bank management shall implement and thereafter adhere to a written program to effectively assess and manage the risks posed by third-party fintech relationships ("Third-Party Risk Management Program"). Refer to OCC Bulletin 2013-29, "Third-Party Relationships" and OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"; Refer to OCC Bulletin 2021-40, "Third-Party Relationships: Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks".

(2) The Third-Party Risk Management Program shall be commensurate with the level of risk and complexity of the Bank's third-party fintech relationship partners and shall, at a minimum, address the following for the Bank's third-party fintech relationship partners:

(a) written policies, procedures, and processes governing the Bank's third-party fintech relationship partners that, at a minimum: (i) address how the Bank identifies and assesses the inherent risks of the products, services, and activities performed by the third-parties, including but not limited to BSA, compliance, operational, liquidity, counterparty and credit risk as applicable; (ii) details how the Bank selects, assesses, and oversees third-parties; (iii) details the Bank's strategic plan for providing necessary resources, infrastructure, technology controls, and organizational capabilities to manage the third-party fintech

relationship partners in a safe and sound manner; and (iv) establishes criteria for Board review and approval of third-party fintech relationship partners;

(b) an assessment of BSA risk for each third-party fintech relationship partner, including risk associated with money laundering, terrorist financing, and sanctions risk as well as the third-party's processes for mitigating such risks and complying with applicable laws and regulations;

(c) due diligence and risk assessment criteria for selecting and approving a third-party fintech relationship partner that is appropriate and unique to the particular products, services, and activities provided by the third-party; Refer to OCC Bulletin 2021-40, "Third-Party Relationships: Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks";

(d) an effective compliance oversight program for third-party fintech relationship partners to include: (i) evaluation of the products, services, and activities offered through the Bank's third-party fintech relationship partners for compliance with applicable laws and regulations; (ii) an effective internal compliance monitoring program; and (iii) a process for addressing any third-party fintech relationship partner's activities identified as non-compliant or in violation of applicable laws and regulations;

(e) ongoing monitoring of third-party fintech relationship partner's activities and performance;

(f) contingency plans for terminating third-party fintech relationships in an effective manner;

(g) documentation, management information systems ("MIS"), and reporting

that facilitates Board and management oversight, accountability, monitoring, and risk management associated with third-party fintech relationships;

(h) an audit plan for independent reviews by a qualified auditor who is independent of day-to-day operations that allows Bank management to assess whether the Bank's risk management practices align with the Bank's policies, procedures, and processes. The audit plan must provide for effective independent reviews to assess internal controls as well as IT, compliance, and operational risk associated with third-party fintech relationships;

(i) a written assessment from a qualified, independent certified public accountant to ensure the accounting for transactions initiated through the fintech partnerships conform with GAAP and financial reporting is in line with contractual terms; and

(j) evaluation and implementation of adequate staffing across the third-party fintech relationship line of businesses to ensure the oversight and management of the third-party fintech relationship line of businesses is properly staffed with personnel with the requisite expertise to oversee and manage the risks associated with the third-party fintech relationship line of businesses.

(3) Prior to onboarding new third-party fintech relationship partners, signing a contract with a new fintech partner, or offering new products or services or conducting new activities with or through existing third-party fintech relationship partners, the Board shall obtain no supervisory objection from the OCC. At a minimum, the bank shall submit the due diligence package including supporting documentation, any proposed contract, and any management or board committee minutes approving the relationship.

(4) The Board shall review the effectiveness of the Third-Party Risk Management Program at least annually, and more frequently if necessary or if required by the OCC in writing, and amend the Third-Party Risk Management Program as needed or directed by the OCC.

#### ARTICLE IV

##### BANK SECRECY ACT RISK ASSESSMENT

(1) Within ninety (90) days of the date of this Agreement, the Board shall adopt and Bank management shall implement and adhere to an effective written Bank Secrecy Act Risk Assessment Program (“BSA Risk Assessment Program”). The BSA Risk Assessment Program shall ensure BSA compliance risk assessments provide a comprehensive and accurate assessment of the Bank’s BSA compliance risk across all products, services, customers, entities, and geographies, (collectively, “activities”), including all activities provided by or through the Bank’s third-party fintech relationship partners, and shall include, at a minimum:

- (a) revised and updated policies, procedures, and processes designed to identify, measure, monitor, control, and manage the BSA/AML and Office of Foreign Assets Control (“OFAC”) risk, including risk arising from the Bank’s third party fintech relationships;
- (b) inclusion of sufficient analysis and documentation to identify (i) the quantity of risk associated with fintech partner activities, (ii) any control weaknesses and gaps, (iii) any deficiencies identified during independent testing, and (iv) mitigating factors related to identified weaknesses; and
- (c) policies and procedures for developing accurate MIS reporting, including a Money Laundering Risk report, that provides sufficient information to identify

and manage money laundering, terrorist financing, and other illicit finance risks related to the Bank's third-party fintech relationships.

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

## ARTICLE V

### BSA AUDIT PROGRAM

(1) Within ninety (90) days from the date of this Agreement, the Board shall adopt a revised independent BSA audit program ("BSA Audit Program") that includes an expanded scope and risk-based review of activities conducted through the Bank's third-party fintech relationships. The BSA Audit Program shall, at a minimum, be sufficient to:

- (a) establish an audit plan for independent reviews by a qualified auditor independent from day-to-day operations;
- (b) determine the Bank's compliance with applicable laws, rules, and regulations;
- (c) connect the BSA risk assessment to the scope of audit work performed;
- (d) evaluate the Bank's adherence to established policies, procedures, and processes, with particular emphasis directed to the Bank's adherence to its policies for BSA/AML and OFAC compliance; and
- (e) establish sufficient transaction testing to validate the effectiveness of suspicious activity monitoring processes.

(2) All audits conducted by the internal or external auditor shall be engaged by, reviewed, and approved by the Audit Committee. All reports prepared by internal or external

auditors shall be submitted in writing directly to the Audit Committee and reviewed by the Board.

(3) No less than quarterly, the Board or Audit Committee must review any outstanding BSA audit findings and ensure that corrective actions noted in the BSA audit reports are completed in a timely manner.

## ARTICLE VI

### BANK SECRECY ACT COMPLIANCE PERSONNEL

(1) Within ninety (90) days of the date of this Agreement, the Board shall ensure that the Bank's BSA Department is appropriately staffed with personnel that have requisite expertise, training, skills, and authority. The Board shall ensure that the Bank maintains 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.

(2) Within ninety (90) days of this Agreement, the Board shall review and assess the capabilities and qualifications of the Bank's BSA Officer and BSA Department staff to perform present and anticipated duties, and determine whether changes will be made, including but not limited to, the need for additions to current BSA Department staff.

(3) In the event that the BSA Officer position is vacated, the Board shall provide written notice to the OCC within thirty (30) days of such vacancy and 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 Agreement and the safe and sound operation of



functions within the scope of that position's responsibility.

## ARTICLE VII

### CUSTOMER DUE DILIGENCE, ENHANCED DUE DILIGENCE, AND HIGH RISK CUSTOMER IDENTIFICATION

(1) Within ninety (90) days of the date of this Agreement, the Board shall adopt, and Bank management shall implement and adhere to revised and expanded risk-based policies, procedures, and processes ("Program") to obtain and analyze appropriate customer due diligence ("CDD"), enhanced due diligence ("EDD"), and beneficial ownership ("BO") information for all bank customers at the time of account opening and on an ongoing basis, and to effectively use this information to monitor and investigate, suspicious or unusual activity. The Program, at a minimum, must include for the fintech business:

- (a) written risk-based policies and procedures for conducting ongoing CDD to enable the Bank to: (i) identify, assess, and evaluate the Bank's customers for purposes of compliance with the BSA; (ii) develop CDD processes that are commensurate with the Bank's BSA/AML risk profile with increased focus on higher risk customers and customer transactions; (iii) understand the nature and purpose of the customer relationship in order to develop a customer risk profile; (iv) collect, maintain, and update customer information for all customers, including information regarding the beneficial owner(s) of legal entity customers; (v) use customer information and the customer risk profile to understand the types of transactions a particular customer would be expected to engage in, and as a baseline against which suspicious transactions are identified; and (vi) conduct ongoing monitoring for the purpose of identifying and reporting suspicious

transactions.

(b) effective processes for developing customer risk profiles that identify specific risks of individual customers or categories of customers;

(c) policies and procedures that define management and staff responsibilities for CDD, including authority and responsibility for decisions to open higher risk accounts and for reviewing and approving changes to a customer's risk profile, as applicable;

(d) policies, procedures, and processes to identify customers that may pose higher risk for money laundering or terrorist financing that include whether and/or when, on the basis of risk, it is appropriate to obtain and review additional customer information such as customer's products, services, and customers;

(e) policies, procedures, and processes for documenting the Bank's analysis associated with the due diligence process, including the process for resolving issues when insufficient or inaccurate information is obtained;

(f) policies, procedures, and processes for determining how customer information, including beneficial ownership information for legal entity customers, is used to meet relevant regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of banking accounts, and determining OFAC sanctioned parties.

(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.

## ARTICLE VIII

### SUSPICIOUS ACTIVITY MONITORING AND REPORTING PROGRAM

(1) Within ninety (90) days of the date of this Agreement, the Board shall ensure Bank management develops, implements, and adheres to an enhanced written risk-based program, pursuant to 12 C.F.R. § 21.11, to ensure the timely identification, analysis, and suspicious activity monitoring and reporting for all lines of business, including activities provided by and through the Bank's third-party fintech relationship accounts and sub-accounts ("Suspicious Activity Monitoring and Reporting Program").

(2) The Suspicious Activity Monitoring and Reporting Program shall include, at a minimum, for the Bank's fintech third-party relationship partners:

- (a) an assessment/evaluation of the effectiveness of the Bank's existing policies and procedures for suspicious activity monitoring and reporting including the effectiveness of the Bank's existing automated system for suspicious activity monitoring;
- (b) revised and updated policies and procedures for review and documentation of suspicious activity that are commensurate with the Bank's risk profile, with an action plan for the Bank to address any deficiencies and weaknesses identified with suspicious activity monitoring and reporting;
- (c) procedures and processes for the Bank to quantify the volume of activities and transactions conducted by or through each of the Bank's third-party fintech relationship accounts and sub-accounts;

(d) procedures and processes that include a review for suspicious activity of cash transactions, ACH, and wire activity conducted through the Bank; and

(e) independent model validation of the Bank's automated system for suspicious activity monitoring after enhancements are made to address concerns related to suspicious activity monitoring of activities generated by or through the Bank's third-party fintech relationship accounts and sub-accounts.

(3) The Board shall review the effectiveness of the Suspicious Activity Monitoring and Reporting Program periodically, at a minimum annually, and amend the Suspicious Activity Monitoring and Reporting Program as needed or directed by the OCC.

## ARTICLE IX

### SUSPICIOUS ACTIVITY REVIEW LOOKBACK

(1) Within thirty (30) days of the date of this Agreement, the Bank shall submit to the Assistant Deputy Comptroller, for review and prior written determination of no supervisory objection, an action plan ("Action Plan") to conduct a review and provide a written report of the Bank's suspicious activity monitoring ("SAR Look-Back"). The purpose of the SAR Look-Back is to determine whether Suspicious Activity Reports ("SAR") should be filed for any previously unreported suspicious activity pursuant to 12 C.F.R. § 21.11. The scope of the SAR Look-Back shall include high risk customer activity involving the Bank's third-party fintech relationship partners.

(2) Upon receipt of no supervisory objection to the Action Plan, the Bank shall implement the Action Plan and complete the SAR Look-Back within the proposed timeframe. Upon completion of the SAR Look-Back, the Bank shall provide a report to the Board, with a

copy to the OCC, of any previously unreported suspicious activity identified during the SAR Look-Back and file SARs in accordance with 12 C.F.R. § 21.11. The SAR Look-Back report should also 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 that warranted SAR filings or modifications to existing SAR filings; and
- (e) the number of customers where the Bank determined not to file a SAR.

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

## ARTICLE X

### INFORMATION TECHNOLOGY CONTROL PROGRAM

(1) Within ninety (90) days of the date of this Agreement, Bank management shall implement and adhere to an acceptable written program to effectively assess and manage the Bank's information technology ("IT") activities, including those activities conducted through and by the Bank's third-party fintech relationship partners ("IT Control Program").

(2) The IT Control Program shall be commensurate with the level of risk and complexity of the Bank's IT activities, including those activities conducted through the Bank's third-party fintech relationship partners, and shall, at a minimum, address the following:

- (a) an updated effective IT risk governance program that establishes the roles, responsibilities, and accountability of the Board of directors and management and includes Board oversight of the information technology risk management of the Bank's third-party fintech relationship partners;
- (b) an updated effective IT risk assessment process that includes: identification and measurement of risks to information and technology assets, within the Bank and/or controlled by third-party fintech 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;
- (c) an updated effective written program with standards and controls over data structure, usage, and storage, including customer data processed and controlled by the Bank's third-party fintech relationship partners;
- (d) an updated written, Board-approved, enterprise-wide business continuity management and resiliency process that includes processes and systems for the Bank's third-party fintech relationship partners ("Business Continuity Plan"); the Business Continuity Plan shall include 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; and
- (e) an annual information security program report to the Board that includes a review and analysis of information technology security and risk management

related to activities conducted through and by the Bank's third-party fintech relationships.

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

## ARTICLE XI

### GENERAL BOARD RESPONSIBILITIES

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

(2) In each instance in which this Agreement 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 Agreement;

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

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

- (d) hold Bank management and personnel accountable for executing their duties and responsibilities pertaining to or resulting from this Agreement;
- (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 Agreement; and
- (f) address any noncompliance with corrective actions in a timely and appropriate manner.

## ARTICLE XII

### OTHER PROVISIONS

- (1) As a result of this Agreement, the Bank is not:
  - (a) precluded from being treated as an “eligible bank” for the purposes of 12 C.F.R. Part 5, unless the Bank fails to meet any of the requirements contained in subparagraphs (1) – (4) of 12 C.F.R. § 5.3, Definitions, *Eligible bank or eligible savings association*, or is otherwise informed in writing by the OCC;
  - (b) 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, unless the Bank is otherwise subject to such requirements pursuant to 12 C.F.R. § 5.51(c)(7)(i) and (iii); and
  - (c) precluded from being treated as an “eligible bank” for the purposes of 12 C.F.R. Part 24, unless the Bank fails to meet any of the requirements



contained in 12 C.F.R. § 24.2(e)(1)-(3) or is otherwise informed in writing by the OCC.

(2) This Agreement supersedes all prior OCC communications issued pursuant to 12 C.F.R. §§ 5.3, 5.51(c)(7)(ii), and 24.2(e)(4).

### ARTICLE XIII

#### CLOSING

(1) This Agreement is intended to be, and shall be construed to be, a “written agreement” within the meaning of 12 U.S.C. § 1818, and expressly does not form, and may not be construed to form, a contract binding on the United States, the OCC, or any officer, employee, or agent of the OCC. Notwithstanding the absence of mutuality of obligation, or of consideration, or of a contract, the OCC may enforce any of the commitments or obligations herein undertaken by the Bank under its supervisory powers, including 12 U.S.C. § 1818(b)(1), and not as a matter of contract law. The Bank expressly acknowledges that neither the Bank nor the OCC has any intention to enter into a contract. The Bank also expressly acknowledges that no officer, employee, or agent of the OCC has statutory or other authority to bind the United States, the U.S. Treasury Department, the OCC, or any other federal bank regulatory agency or entity, or any officer, employee, or agent of any of those entities to a contract affecting the OCC’s exercise of its supervisory responsibilities.

(2) This Agreement 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 Agreement shall mean calendar days and the computation of any period of time imposed by this Agreement shall not include the date of the act or event that commences the period of time.

(3) The provisions of this Agreement shall remain effective and enforceable 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 Agreement, the Board or a Board-designee shall submit a written request to the Assistant Deputy Comptroller asking for the desired relief. Any request submitted pursuant to this paragraph shall include a statement setting forth in detail the special circumstances that warrant the desired relief or prevent the Bank from complying with the relevant provision(s) of the Agreement, 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.

(4) The Bank will not be deemed to be in compliance with this Agreement until it has adopted, implemented, and adhered to all of the corrective actions set forth in each Article of this Agreement; 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 to demonstrate the sustained effectiveness of the corrective actions.

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

(6) 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 enter into this Agreement.

(7) All reports, plans, or programs submitted to the OCC pursuant to this Agreement shall be forwarded via BankNet, to the following:

Amanda Edwards, Assistant Deputy Comptroller  
Office of the Comptroller of the Currency  
Roanoke Field Office

(8) The terms of this Agreement, 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/

---

Amanda Edwards, Assistant Deputy Comptroller  
Office of the Comptroller of the Currency  
Roanoke Field Office



/s/

---

Randolph N. Reynolds, Jr., Director

/s/

---

C. Frank Scott, III, Director

/s/

---

Vance Spilman, Director

/s/

---

William W. Stokes, Director

/s/

---

Carolyn J. Woodruff, Director

8-17-22

---

Date

8-17-22

---

Date

8-17-22

---

Date

8-17-2022

---

Date

8-17-2022

---

Date