FEDERAL DEPOSIT INSURANCE CORPORATION

WASHINGTON, D.C.

In the Matter of GUNNISON VALLEY BANK GUNNISON, UTAH (INSURED STATE NONMEMBER BANK)	CONSENT ORDER FDIC-18-0187b

The Federal Deposit Insurance Corporation ("FDIC") is the appropriate Federal banking agency for Gunnison Valley Bank, Gunnison, Utah ("Bank") under Section 3(q) of the Federal Deposit Insurance Act ("FDI Act"), 12 U.S.C. § 1813(q)(3). 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 December 11, 2018, that is accepted by the FDIC. With the Stipulation, the Bank has consented, without admitting or denying any charges of unsafe or unsound banking practices and/or violations of law relating to the Bank's document preservation practices, Bank Secrecy Act and Anti-Money Laundering program, or Information Technology Program, 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) has been satisfied, the FDIC hereby orders that:

Document Preservation Practices

1. The Bank shall immediately suspend its document disposal and destruction schedule for all records pertaining to electronic, hardcopy, final or draft documents related to the Bank materials concerning:

(a) Financial and accounting records;

(b) Credit files;

(c) Loan portfolios;

(d) Deposit accounts;

(e) E-mails and work files of any former and current finance and accounting personnel and senior executives; and

(f) Communications with or of the Bank's Board of Directors.

2. The Bank shall prevent document disposal and destruction due to routine operations or attempts at deletion.

3. The Bank shall employ proper techniques and protocols to ensure the protection and preservation of documents at the Bank.

4. Concerning documents in the above categories that have already been disposed and/or destroyed, the Bank shall immediately provide the following information to the Regional Director of the FDIC's San Francisco Regional Office with respect to each destroyed document:

(a) Detailed description of the document;

(b) Date of destruction;

(c) Reason for destruction;

(d) Person responsible for the destruction; and

(e) Person who authorized the destruction.

Bank Secrecy Act/Anti-Money Laundering Program

5. Within 90 days of the effective date of this Order, the Bank shall comply in all material respects with the Bank Secrecy Act ("BSA"), 31 U.S.C. § 5311 et seq., 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951-1959, and its implementing regulations, 31 C.F.R. Chapter X,

section 326.8 and Part 353 of the FDIC's Rules and Regulations, 12 C.F.R. § 326.8 and Part 353. In addition, the Bank shall take all necessary steps to ensure future compliance with these laws and regulations.

6. Within 90 days from the effective date of this Order, the Bank shall develop, adopt, and implement an appropriate system of internal controls over the BSA/Anti-Money Laundering ("AML") compliance program. Such internal controls shall include, but not be limited to:

(a) Policies, procedures, and processes tailored specifically to the Bank and its BSA/AML risk profile.

(b) Written procedures will include, at a minimum:

(i) Suspicious activity monitoring and reporting, including expectations with respect to investigations or reviews completed that do not result in the filing of a suspicious activity report;

(ii) Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD") processes, as well as expectations with respect to the identification and ongoing monitoring of high-risk customers; and

(iii) Currency transaction reporting ("CTR") exemptions, including ongoing customer reviews.

7. Within 90 days from the effective date of this Order, the Bank shall establish and implement written procedures to monitor for and appropriately report suspicious activity. At a minimum, the Bank shall take the following actions when establishing and implementing the procedures:

(a) Document the methods by which suspicious activity will be identified, including standards regarding which system reports will be reviewed and how often, staff

responsible for reviewing system reports, and methods used to refer potentially suspicious activity to the BSA Officer or designee; and

(b) Detail the process of maintaining documentation of suspicious activity investigations, including detailed rationale and support when the investigation does not result in the filing of a suspicious activity report.

8. Within 90 days from the effective date of this Order, the Bank shall establish and implement written, risk-based CDD and ongoing due diligence procedures. At a minimum, the Bank shall take the following actions when establishing and implementing the procedures:

(a) Establish standards regarding what information will be requested of, and collected from, new customers;

(b) Establish BSA/AML risk profiles for all new customers, and specify methods used to establish such risk profiles, including details of any customer risk scoring system, as applicable;

(c) Define "high risk" customer or account formally in policy and procedures;

(d) Document in procedures how management will compare expected customer activity to actual activity on an ongoing basis, using a risk-based approach (i.e. for customers internally identified as posing higher-than-normal BSA/AML risk);

(e) Document in procedures and fully implement in practice the processes for collecting and verifying business entity customer information, including beneficial ownership information for business entity customers, according to 31 C.F.R. § 1020.210(b)(5) and any other applicable BSA regulations; and

(f) Establish guidelines and administer training on monitoring for and reporting unusual or suspicious activity based on the results of ongoing customer activity reviews:

(i) Ongoing customer activity reviews should be risk-based, according to the Bank's own policy and procedures, thus focusing on those customers who pose higher-than-normal BSA/AML risk when considering customer and/or account type, products/services used, transactions processed, and geographic locations;

(ii) Ongoing customer activity review documentation should include support for the reasonableness of the type and volume of customer transactions, based on the customers' BSA/AML risk profiles; and

(iii) Ongoing customer activity reviews resulting in the identification of suspicious activity should be reported according to 12 C.F.R. Part 353.

9. Within 90 days from the effective date of this Order, the Bank shall establish and implement written procedures for appropriately managing customers that have been exempted from CTR filing. At a minimum, the written procedures shall include the following:

(a) The process by which annual account/customer reviews will be conducted, including the maintenance of documented evidence of such reviews; and

(b) The process by which periodic suspicious activity account reviews for all CTR-exempted customers.

10. Within 90 days from the effective date of this Order, the Bank shall establish an appropriate independent testing function for the review of the BSA/AML compliance program. At a minimum, the Bank shall take the following actions:

(a) Execute a formal engagement/agreement prior to the completion of the BSA/AML independent review;

(b) Ensure that the independent review of the BSA/AML program is appropriate by sufficiently detailing expected review procedures within review engagement

documentation. BSA/AML program independent reviews should include, at a minimum, review and analysis of the following elements:

(i) Completeness and appropriateness of the BSA/AML and Office of Foreign Assets Control ("OFAC") risk assessment(s);

(ii) Effectiveness of management's system of internal controls over the BSA/AML compliance program, including suspicious activity monitoring and reporting;

(iii) Performance and adequacy of the BSA Officer and supporting staff; and

(iv) Scope and effectiveness of the BSA/AML training program.

(c) Ensure that the firm/individual fulfilling the independent BSA/AML testing function possesses the requisite experience and expertise to perform the review.

11. Within 90 days from the effective date of this Order, the Bank shall perform (or contract to be performed) a BSA/AML program evaluation, part of which will include an evaluation of the Bank's staff dedicated to performing or overseeing BSA/AML compliance. The Bank shall subsequently take appropriate actions based on the results of the program and staffing evaluation.

12. Within 90 days from the effective date of this Order, the Bank shall take the following actions to further enhance the OFAC compliance program:

(a) Improve OFAC-related policies and procedures by:

(i) Addressing explicitly in policy the Board's OFAC risk tolerance, including the required frequency of ongoing OFAC scrubs (i.e. daily, weekly, monthly, annually, whenever OFAC lists are updated, etc.); and

(ii) Ensuring that practices align with the updated OFAC policy, i.e. conducting ongoing OFAC screening as often as the Board deems appropriate.

(b) Complete an OFAC risk assessment, either as part of or separately from, the BSA/AML risk assessment; and

(c) Create and maintain documentation of clearing all false positive OFAC alerts when opening new accounts or during periodic OFAC scrubs.

Information Technology Program

13. Within 90 days of the effective date of this Order, the Bank shall develop and implement an Information Technology ("IT") audit program that meets regulatory requirements. The Bank's IT audit program shall:

(a) Identify areas of greatest IT risk exposure to the Bank in order to focus audit resources;

(b) Promote the confidentiality, integrity, and availability of information systems;

(c) Determine the effectiveness of management's planning and oversight of IT activities;

(d) Evaluate the adequacy of operating processes and internal controls;

(e) Require appropriate corrective action to address deficient internal controls and follow up to ensure management promptly and effectively implements the required actions.

14. Within 90 days of the effective date of this Order, the Bank shall ensure compliance with the Gramm–Leach–Bliley Act by strengthening the Bank's written Information Security Policy. The Information Security Policy shall be enhanced to include administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

15. Within 90 days of the effective date of this Order, the Board shall increase its oversight of the IT area, including enhancing the identification, assessment, and management of IT risks and governance. The Board shall ensure that the Bank:

(a) Establishes tracking mechanisms for audit and regulatory exceptions and remediate items on the list in an appropriate timeframe;

(b) Implements appropriate User Access provisioning and oversight;

(c) Performs cybersecurity self-assessments using the FFIEC Cybersecurity Assessment Tool or a similar tool annually;

(d) Further develop and test the disaster recovery plan;

(e) Formalize the vendor management program;

(f) Formalize the patch management program; and

(g) Create a formal wire transfer policy to outline procedures for the wire transfer process.

16. Within 90 days of the effective date of this Order, the Bank shall expand its Information Security Risk Assessment(s) to include potential threats to assets and specific controls in place that mitigate risk for each identified threat.

17. Within 120 days of the effective date of this Order, the Board shall conduct a review of staffing to ensure that adequate IT resources are provided, including an adequate number of employees with required IT skills, knowledge, and experience. The Board shall ensure that the Bank's IT personnel have experience in the various technology systems and platforms deployed in the Bank.

18. Within 90 days of the effective date of this Order, the Bank shall develop and adopt a Red Flags Identity Theft Policy. Thereafter, the Bank shall implement annual written

reporting to the Board on the Bank's identity theft detection program. The Red Flags Identity Policy should:

(a) Identify relevant red flags for covered accounts;

(b) Detect red flags that have been incorporated into the Program;

(c) Respond appropriately to any red flags that are detected; and

(d) Ensure the program (including the red flags determined to be relevant) is updated periodically.

Reporting and Other Requirements

19. Within 90 days of the effective date of this Order, the Bank shall eliminate and/or correct all violations of law identified in the Report of Examination dated March 26, 2018. Additionally, the Bank shall take all necessary steps to ensure future compliance with all applicable laws and regulations.

20. Within 45 days of the end of the first quarter following the effective date of this Order, and within 45 days of the end of each quarter thereafter, the Bank shall furnish written progress reports to the Regional Director and Commissioner of the Utah Department of Financial Institutions ("Commissioner") detailing the form and manner of any actions taken to secure compliance with this Order and the results thereof. Such reports shall include a copy of the Bank's Report of Condition and the Bank's Report of Income. Such reports may be discontinued when the corrections required by this Order have been accomplished and the Regional Director and the Commissioner have released the Bank in writing from making further reports.

21. The Bank's Board shall certify in writing to the Regional Director when all of the above actions have been accomplished. All actions taken by the Board pursuant to this Order shall be duly noted in the minutes of its meetings.

22. During the life of this Order, the Bank shall not establish any new branches or other offices of the Bank without the prior written consent of the Regional Director.

23. Following the effective date of this Order, the Bank shall send to its shareholder(s) or otherwise furnish a description of this Order in conjunction with the Bank's next shareholder communication and also in conjunction with its notice or proxy statement preceding the Bank's next shareholder meeting. The description shall fully describe the Order in all material respects. The description and any accompanying communication, statement, or notice shall be sent to the FDIC, Accounting and Securities Section, Washington, D.C. 20429, at least 15 days prior to dissemination to shareholders. Any changes requested to be made by the FDIC shall be made prior to dissemination of the description, communication, notice, or statement.

The provisions of this Order shall not bar, estop, or otherwise prevent the FDIC, the UDFI, 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).

This Order will become effective upon its issuance by the FDIC.

The provisions of this Order shall be binding upon the Bank, its institution-affiliated parties, and any successors and assigns thereof.

The provisions of this Order shall remain effective and enforceable except to the extent that and until such time as any provision has been modified, terminated, suspended, or set aside by the FDIC.

Violation of any provisions of this Order, will be deemed to be conducting business in an unsafe or unsound manner, and will subject the Bank to further regulatory enforcement action.

Issued pursuant to delegated authority

Dated this 12th day of December, 2018.

/s/

Paul P. Worthing
Deputy Regional Director
Division of Risk Management Supervision
San Francisco Region
Federal Deposit Insurance Corporation