FEDERAL DEPOSIT INSURANCE CORPORATION
WASHINGTON, D.C.

And

MINNESOTA DEPARTMENT OF COMMERCE
ST. PAUL, MINNESOTA

In the Matter of	)	
	)	
Security State Bank of Warroad	)	**CONSENT ORDER**
Warroad, Minnesota	)	
	)	**FDIC-18-0222b**
(Insured State Nonmember Bank)	)	
	)	

The Federal Deposit Insurance Corporation ("FDIC") is the appropriate Federal banking agency for the Security State Bank of Warroad, Warroad, Minnesota ("Bank"), under Section 3(q) of the Federal Deposit Insurance Act (FDI Act), 12 U.S.C. § 1813(q).

Based on the findings of the FDIC examination of the Bank as contained in the September 17, 2018, Report of Examination ("Report of Examination"), the FDIC and the Minnesota Department of Commerce (collectively "Supervisory Authorities"), determined that the requirements for an order under 12 U.S.C. § 1818(b) and Minnesota statutes have been satisfied.

The Bank, by and through its duly elected and acting Board of Directors ("Board"), has executed a "Stipulation and Consent to the Issuance of a Consent Order" ("Stipulation"), dated February 21, 2019. With the Stipulation, the Bank has consented, without admitting or denying any charges of unsafe or unsound banking practices or violations of law or regulation, to the issuance of this Consent Order ("ORDER") by the Supervisory Authorities.

Based on the above, the Supervisory Authorities hereby order the following:

1. Information Technology ("IT")

(a) Within 45 days from the effective date of this ORDER, the Board shall identify and designate an individual or individuals, whether from internal or external sources, with the requisite knowledge, qualifications, and experience, to provide oversight for the information technology function.

(b) Within 60 days from the effective date of this ORDER, the Bank shall improve the risk assessment process for IT to conform to Part 364, Appendix B of the FDIC's Rules and Regulations, 12 C.F.R. Part 364 Appendix B. The risk assessment shall be in written form and at a minimum identify the following:

(i) Board members, committee members, or other designees charged with overseeing the risk assessment process;

(ii) Vulnerabilities and threats by area (for example, business function, hardware, and/or applications maintained in-house or outsourced to service providers), including internal control weaknesses and conflicting duties;

(iii) Likelihood and probability of such threats, taking into consideration natural, intentional, and unintentional causes;

(iv) Methods for mitigating or minimizing threats and risks through administrative, technical, and physical controls;

(v) Written policies containing required risk mitigation methods; and

(vi) Residual risk after mitigating controls are applied.

(c) Within 90 days from the effective date of this ORDER, the Bank shall develop and implement an effective cybersecurity preparedness program that provides for an assessment of the Bank's cybersecurity risk, incorporates cybersecurity threats and mitigation strategies into the information security program, and includes a threat intelligence program to assist in proactively identifying and where possible, mitigating active cybersecurity threats.

(d) Within 120 days from the effective date of this ORDER, the Bank shall complete and implement a written information security program consistent with the requirements and criteria found in Part 364, Appendix B of the FDIC's Rules and Regulations, and include specific and standardized policies and procedures surrounding Board reporting, patch management, business continuity/disaster recovery planning, internet banking, network administration, remote access, user access rights and logical security standards, system activity monitoring, including firewall and intrusion detection technologies, and wire transfer and automated clearinghouse functions.

(e) Within 30 days after completion of (d) above, the Bank shall develop a schedule for training on the information security program, including cybersecurity threats and mitigation strategies for all employees and members of the board. The training schedule should be implemented immediately following completion of the information security program in subparagraph (d) above.

(f) Within 90 days from the effective date of this ORDER, the Bank shall develop a written IT audit program for the purpose of determining compliance with the written information security program. The IT audit program shall:

(i) Be risk-based according to the inherent risk conclusions of the IT risk assessment;

(ii) Identify the scope, type, and frequency of audits to be performed; and,

(iii) Include provisions for Board reporting, audit tracking, and findings resolution.

The Board or designated audit committee shall be responsible for directing and overseeing audit work performed, and for prompt resolution of audit findings.

(g) Within 120 days from the effective date of this ORDER, the Board shall engage a qualified, independent internal or external party to conduct a general controls review and a vulnerability assessment of both the internal and external facing networked environments. The

Board shall take timely corrective actions toward these audit findings in accordance with the audit program developed in subparagraph (f) above.

(h) Within 90 days from the effective date of this ORDER, the Bank shall improve the patch management program by defining roles and responsibilities; inventorying all systems, applications, and firmware that require periodic patch updates; establishing expectations for timelines of patch installation; implementing an effective method, whether automated or manual, internal or outsourced, to identify, test, and apply available patches; and monitoring the program's effectiveness. As part of the patch management program, management shall identify the end of life for all systems, applications, and firmware, and establish and implement a replacement schedule to ensure that all systems are replaced prior to reaching their end of life.

(i) Within 120 days from the effective date of this ORDER, the Bank shall improve the business continuity and disaster recovery plan to address all critical areas of operations, include specific steps to recover and resume business and minimize financial loss, and include emergency response procedures appropriate for the size and complexity of operations. Management shall develop and implement a schedule to regularly validate the effectiveness of the identified recovery strategies including those related to the core, network, and electronic funds transfer functions. Management shall provide employees with initial and periodic training necessary to implement the plan and the plan should be reviewed and approved by the board.

(j) Within 120 days from the effective date of this ORDER, the Bank shall correct each issue identified in the Report of Examination not specifically addressed under subparagraphs (a) – (i) above, including all outstanding prior examination recommendations and audit findings. The Bank shall detail, in written form, actions taken to address each identified issue.

(k) The Board shall submit a progress report to the Supervisory Authorities detailing management's progress toward complying with the above provisions in connection with the requirement for progress reports contained below in this Order.

2. Disclosure of Order to Shareholder

Following the effective date of this ORDER, the Bank shall provide a copy of this ORDER or otherwise furnish a description of this ORDER to its sole shareholder, (i) in conjunction with the Bank's next shareholder communication, and (ii) its notice or proxy statement preceding the Bank's next shareholder meeting.

3. Progress Reports Detailing Compliance with ORDER

(a) Within 30 days of the end of the first calendar quarter following the effective date of this ORDER, and within 30 days of the end of each calendar quarter thereafter, the Bank shall furnish written progress reports to the Supervisory Authorities detailing the form, manner, and results of any actions taken to secure compliance with this ORDER. Such written progress reports shall provide cumulative detail of the Bank's progress toward achieving compliance with each provision of the ORDER, including at a minimum:

(i) descriptions of the identified weaknesses and deficiencies;

(ii) provision(s) of the ORDER pertaining to each weakness or deficiency;

(iii) actions taken or in-process for addressing each deficiency;

(iv) results of the corrective actions taken;

(v) the Bank's status of compliance with each provision of the ORDER; and

(vi) appropriate supporting documentation.

(b) Progress reports may be discontinued when the Supervisory Authorities have, in writing, released the Bank from making additional reports.

MISCELLANEOUS

This ORDER shall be effective on the date of issuance. The provisions of this ORDER shall be binding upon the Bank, its institution-affiliated parties, and any successors and assigns thereof. The provisions of this ORDER shall not bar, estop, or otherwise prevent the FDIC, the Minnesota Department of Commerce, or any other federal or state agency or department from

taking any other action against the Bank or any of the Bank's current or former institution-affiliated parties.

This ORDER is issued and thus effective this 4th day of March, 2019.

MINNESOTA DEPT. OF COMMERCE

/s/
Maxwell Zappia
Deputy Commissioner

FEDERAL DEPOSIT INSURANCE CORP.

/s/
John R. Jilovec
Deputy Regional Director

Communications

All communications regarding this ORDER shall be sent to:

John R. Jilovec
Deputy Regional Director
Federal Deposit Insurance Corporation
1100 Walnut Street, Suite 2100
Kansas City, Missouri 64106

Maxwell Zappia
Deputy Commissioner
Minnesota Department of Commerce
85 7th Place East, Suite 280
Saint Paul, Minnesota 55101

Roderick J. Heneman
President
Security State Bank of Warroad
502 E Lake Street
Warroad, Minnesota 56763