FEDERAL DEPOSIT INSURANCE CORPORATION

WASHINGTON, D.C.

In the Matter of COMENITY SERVICING LLC Columbus, Ohio (SERVICE PROVIDER)	CONSENT ORDER FDIC-23-0066b

The Federal Deposit Insurance Corporation (**FDIC**) is the appropriate Federal regulatory agency for Comenity Servicing LLC (**SP**), under section 3(q) of the Federal Deposit Insurance Act (Act), 12 U.S.C. § 1813(q). The SP provides information technology (**IT**) and other services to certain "insured depository institutions" (**IDIs**) within the meaning of 12 U.S.C. § 1813(c)(2) (**IDIs**) and is an "institution-affiliated party" of those IDIs within the meaning of 12 U.S.C. § 1813(u).

The SP, by and through its duly elected and acting board of managers (Board), has executed a STIPULATION AND CONSENT TO THE ISSUANCE OF A CONSENT ORDER (CONSENT AGREEMENT), dated November 20, 2023, that is accepted by the FDIC. With the CONSENT AGREEMENT, the SP has consented, without admitting or denying any charges of unsafe or unsound practices relating to, among other things, deficiencies and weaknesses in the SP's systems development, project management, business continuity management, cloud operations, and the oversight of business arrangement between the SP and another entity, by contract or otherwise, including any business arrangements with an entity conducting one or more activities for or on behalf of the SP and any party performing these services, or a

component of these services, for or on behalf of such entity (collectively, **Third-Party Relationships**), to the issuance of this CONSENT ORDER (**ORDER**) by the FDIC.

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

I. BOARD REQUIREMENTS

A. Supervision, Direction, Oversight, and Monitoring. The Board must immediately and appropriately increase, commensurate with the size of the SP and the nature, scope, and risk of the SP's activities, whether conducted directly by the SP or through Third-Party Relationships (collectively, **SP Activities**), its supervision and direction of management, and its oversight and monitoring of all SP Activities. The Board must also, at a minimum:

1. *Board Process*: immediately assume full responsibility for the approval, implementation, and adherence to sound standards, policies, procedures, and processes (collectively, **Procedures**) reasonably designed to assure SP Activities, including its provision of IT services to the IDIs, are conducted in a safe and sound manner; ensure complete and timely compliance with this ORDER; and ensure it receives all of the information and documentation, including reports from the Executive Oversight Committee, the establishment of which is required by Paragraph I.A.2. of this ORDER, necessary to fulfill its duties and responsibilities under this ORDER and establish a satisfactory process to do so (**Board Process**). The Board Process must include, at a minimum:

a. meeting at least monthly to monitor the SP Activities along with the SP's overall condition and risk profile; review compliance with this ORDER, Board-

approved Procedures and plans, and any compliance exceptions; and provide direction to the Executive Oversight Committee with respect to any action necessary regarding an identified risk or compliance exception or that is otherwise necessary to ensure SP Activities are conducted in a safe and sound manner; and

b. engaging in robust discussions as part of all Board meetings, and comprehensively and accurately documenting those discussions in meeting minutes, including a satisfactory summary of matters reviewed, discussion of expectations and any challenges or questions, any specific actions taken or to be taken as a result of these discussions, including any requirements of or directions to SP management, and the names of any dissenting managers to such actions;

2. *Executive Oversight Committee*: establish, within 30 days from the effective date of this ORDER, an oversight committee of SP executive officers (**Executive Oversight Committee**) with the appropriate experience, expertise, and proficiency with respect to SP Activities to oversee and ensure that the SP complies with the requirements of this ORDER and conducts SP Activities in a safe and sound manner. The Executive Oversight Committee must, at a minimum:

a. have a charter and/or other organizational documents, including Procedures (collectively, Organizational Documents) that clearly sets forth the duties, responsibilities, and authority of the Executive Oversight Committee;

b. meet no less frequently than monthly to review and assess the SP's overall condition and risk profile; status of actions necessary to ensure timely compliance with this ORDER, Board-approved Procedures, and plans; any compliance exceptions; and any action necessary to appropriately mitigate or address an identified risk or compliance exception or that

is otherwise necessary to ensure SP Activities are conducted in a safe and sound manner;

c. engage in robust discussions as part of all Executive Oversight Committee meetings, and comprehensively and accurately document those discussions in meeting minutes, including a satisfactory summary of matters reviewed, discussion of expectations and any challenges or questions, any specific actions taken or to be taken as a result of these discussions, including any requirements of or directions to SP management, and the names of any dissenting managers or executive officers to such actions; and

d. prepare and provide to the Board one or more appropriately detailed reports regarding (i) the overall condition of the SP; (ii) identified risks and action to be taken to appropriately mitigate or address such risk; (iii) the status of corrective action required by this ORDER; and (iv) the SP's compliance with Board-approved Procedures or plans, any compliance exceptions or delays, and the action the Executive Oversight Committee will take to address any exceptions or delays;

3. *System Conversions:* ensure that the SP does not initiate, including the entry into any binding commitment or written agreement involving a Third-Party Relationship, a system conversion project that is rated "Deluxe" under the SP's project complexity scorecard methodology in place as of the effective date of this Order (**Large and Complex System Conversion**) without first obtaining Board attestation to the readiness of the SP to undertake such a project. The Board must submit to the FDIC Deputy Regional Director (**DRD**) a notification of a planned Large and Complex System Conversion (**System Conversion Notification**) as a PDF document through the FDIC's Secure Email portal (securemail.fdic.gov) using e-mail address: NYMailRoom@fdic.gov. The System Conversion Notification must, at a minimum, include an initial thorough and well-documented review and assessment of the risks

associated with the proposed Large and Complex System Conversion; a written assessment and recommendation of the actions necessary to satisfactorily mitigate identified risks; written recommendations for the establishment of Procedures, including policy parameters, for the conversion, including testing, monitoring, escalation, and reporting Procedures; draft agreements for any Third-Party Relationship involved with the proposed Large and Complex System Conversion; and the Board's written attestation that the SP has a comprehensive and appropriate plan in place to effectively manage and execute the Large and Complex System Conversion;

4. *Risk Management Framework:* ensure that the SP has a proactive, effective risk management framework, including Procedures for systems development, project management, management of Third-Party Relationships, business continuity management, and cloud operations, that appropriately identifies and assesses risks, establishes and monitors the effectiveness of controls established to mitigate such risks, and enables the SP to conduct SP Activities in a safe and sound manner and in compliance with applicable laws and regulations (collectively, **Risk Management Framework**);

5. *Personnel and Resources:* ensure that the SP maintains personnel, including officers, managers, and staff, with appropriate experience and expertise and sufficient authority, independence, and suitable resources to enable the satisfactory implementation of the Risk Management Framework and assure SP Activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations;

6. *SP Activity Risk Reporting:* ensure adequate information systems and Procedures are in place to provide the Board and the Executive Oversight Committee with

timely, relevant, and accurate information regarding risks related to SP Activities in a consistent and readily understandable format at regular intervals;

7. *Executive Oversight Committee and Management Expectations and Monitoring:* set clear and measurable expectations for the Executive Oversight Committee and management regarding their (a) leadership across business lines and operations; (b) sound and consistent governance of the Risk Management Framework; (d) oversight and monitoring of Third-Party Relationships; (e) maintenance of risks within the Board's risk appetite parameters and established risk limits; and (f) establish and maintain Procedures to monitor and regularly evaluate Executive Oversight Committee and management adherence to these Board expectations and ensure appropriate revisions are timely made to assure SP Activities are conducted in a safe and sound manner and in compliance with applicable law and regulations;

8. *IT Audit:* ensure the SP's internal IT audit function (**IT Audit**) (a) is appropriate to the size of the SP and the nature and scope of SP Activities; (b) appropriately considers available risk assessments, studies, reports, including the August 29, 2022 FDIC IT Report of Examination (**2022 Report**) and other regulatory findings, plans, and/or Procedures related to SP Activities in its audit risk-assessment process; and (c) appropriately assesses the SP's implementation of and adherence to the Risk Management Framework and any other Procedures or plans adopted by the Board; and

9. *Risk Management Framework Tracking Procedures:* establish and maintain Procedures to track corrective, preventive, and/or remedial actions addressing identified deficiencies and weaknesses in the Risk Management Framework to ensure such corrective

actions are implemented in a timely manner, and thereafter monitor implementation of and adherence to resulting revisions to the Risk Management Framework by the SP.

B. Corrective Action. The Board must also ensure that the SP immediately takes all steps necessary, consistent with other provisions of this ORDER and safe and sound practices, to:

1. continue to correct and prevent the recurrence of any unsafe or unsound practices, including Examination Concerns Requiring Attention (**ECRAs**) identified in the 2022 Report; and

2. fully comply with the provisions of this ORDER in a timely manner.

II. SP PROCEDURES

The Board must ensure that the SP has Procedures in place that (i) are commensurate with its size and the nature, scope, and risk of SP Activities and satisfactorily provide an organizational structure with clear lines of authority and responsibility for monitoring adherence to established Procedures, effective risk assessment, timely and accurate reporting, and conducting SP Activities in a safe and sound manner and in compliance with applicable laws and regulations; and (ii) include appropriate Procedures for each of the areas listed in subparagraph A below that proactively and effectively assure all SP Activities are conducted in a safe and sound manner and comply with applicable laws and regulations. The Board must also ensure that the Procedures are (i) reviewed and assessed in accordance with subparagraph A as of the date on which the reviews and assessments commence and that the reviews and assessments appropriately consider the ECRAs and other deficiencies and weaknesses identified in the 2022 Report; (ii) revised and improved in accordance with subparagraph B below; (iii) adopted within

the timeframes established in the SP Revision Plan required by subparagraph B below and appropriately reflected in the Board minutes; and (iv) implemented and adhered to as adopted.

A. SP Report. Within 120 days from the effective date of this ORDER, the SP must complete and submit a written report (**SP Report**) to the DRD and IT Audit reflecting the findings of the reviews and assessments of the areas listed below (**SP Assessments**) with a satisfactorily detailed analysis of each such area identifying any deficiencies, weaknesses, gaps, risk areas, or other issues or concerns and recommended additions, changes, or enhancements to address the findings and ensure SP Activities are conducted in a safe and sound manner and in compliance with all applicable laws and regulations. The SP Assessments must, at a minimum, appropriately consider the size of the SP and the nature, scope, and risk of SP Activities; the ECRAs; and the other deficiencies and weaknesses identified in the 2022 Report, and include the following areas:

1. *SD Program*: a review of the adequacy and effectiveness of the SP's systems development program (**SD Program**) and related Procedures, including Procedures relating to risk metrics, such as key performance indicators and key risk indicators; establishment and adherence to standards related to decision-making, design and architecture, development and coding, testing, quality assurance, exception management, key metrics, and documentation; testing parameters; testing environment; Third-Party Relationship monitoring and oversight; escalation; and reporting and whether such Procedures enable the SP to safely and prudently develop and implement new systems or enhance existing systems;

2. *PM Program*: an assessment of the adequacy and effectiveness of the SP's project management program (**PM Program**) and related Procedures, including Procedures related to risk pillars, including risk thresholds, risk event triggers, stage gates, and key metrics;

delegated authority; contingency planning; risk acceptances; defect management; Third-Party Relationship monitoring and oversight; escalation; and reporting and whether such Procedures enable the SP to safely and prudently manage projects;

3. *IT RCSA Program*: an assessment of the adequacy and effectiveness of the SP's IT risk and control self-assessment program (**IT RCSA Program**) and related Procedures, including Procedures related to the identification, assessment, and appropriate mitigation of risks associated with IT-centric processes, including cloud processes; Third-Party Relationship monitoring and oversight; escalation; and reporting and whether such Procedures enable the SP to appropriately identify, assess, and mitigate IT risk;

4. *CP Activities Program*: an assessment of the adequacy and effectiveness of the SP's cloud platform activities program (**CP Activities Program**) and related Procedures, including Procedures relating to establishing and adhering to risk metrics and performance and/or operational standards for the SP's cloud platforms, including those related to coding, design and configuration, risk management, reliability and availability, cloud patch management metrics and standards, and compliance with applicable laws, regulations, and Procedures; testing, including stress testing, the adequacy and suitability of the testing platform and environment, and validation of testing results; identification, reporting, and escalation of issues, including those related to development, performance, and/or operation of the SP's cloud platforms, including cloud patch management; monitoring and assessment of cloud development and maturity, including the SP's roadmap documenting its cloud platform strategies, goals, action items, including cloud patch management, timing requirements, and documentation in support of the roadmap; and whether the CP Activities Program and corresponding Procedures enable the SP to appropriately identify, assess, and mitigate cloud platform activity risk;

5. *Business Continuity Governance*: a review of the SP's business continuity and disaster recovery related Procedures, including Procedures related to the networks, systems, cloud platforms, devices, software, hardware, and/or any other information resources, tools, or mechanism used or relied on by the SP to provide IT services to the IDIs; resilience and contingency planning, including backup and recovery strategies; identification, reporting, and escalation of issues; delegation of authority; establishment of and adherence to Procedures; and documentation to assess whether Procedures are adequate to ensure complete and timely compliance with this ORDER;

6. *Staffing and Training*: (a) a review of the current type, number, and expertise of staff and managers assigned to the business continuity and cloud platform areas to assess whether they are adequate to ensure complete and timely compliance with this ORDER and ensure SP Activities are conducted in a safe and sound manner and in compliance with all applicable laws and regulations noting the duties and responsibilities attributable to each position, with a clear and concise description of the relevant knowledge, skills, abilities, certifications, and experience necessary for each position, including delegations of authority, reporting lines, and performance objectives, and detailing any vacancies and additional needs, including those necessary for succession planning; and (b) a review of the training provided to all personnel, including officers, managers, and staff, assigned to the business continuity and cloud platform areas to assess whether it is adequate to ensure complete and timely compliance with this ORDER; and

7. *Information Security*: (a) a review of the risks posed to security, confidentiality, and integrity (collectively, **Information Security Risks**) of the consumer information and customer information (for purposes of this ORDER, the terms "consumer

information" and "customer information" have the meanings ascribed to them in the *Interagency Guidelines Establishing Information Security Standards*, Appendix B to 12 C.F.R. part 364) of the IDIs to which the SP provides IT services, identifying and describing in appropriate detail each type of consumer and/or customer information reviewed; the medium(s) or form(s), including textual, numerical, graphic, cartographic, narrative, or audiovisual, in which it is found; each location where it is found; how and where such information moves in the SP's and/or an IDI's systems or platforms; and the security measure(s) associated with each type of consumer and/or customer information and how it is tracked to assess whether current Procedures related to information security risks appropriately and effectively identify risks posed and ensure SP Activities are conducted in a safe and sound manner and in compliance with all applicable laws and regulations; (b) a review of how various assessments pertaining to Information Security Risks are collected and aggregated, the SP personnel who are responsible for collecting and aggregating these assessments, and how identified Information Security Risk is escalated, reported, and mitigated to assess whether current Procedures related to Information Security Risk appropriately and effectively collect and aggregate identified Information Security Risks.

B. SP Revision Plan: Within 30 days from the completion of the SP Report, the SP must develop a written plan of action (**SP Revision Plan**) appropriately addressing each recommendation contained in the SP Report with a time frame for completing and implementing the recommended action. The SP must fully implement the SP Revision Plan and provide updates on the implementation status in the Progress Reports required by Paragraph III of this ORDER and to the Executive Oversight Committee and IT Audit.

III. PROGRESS REPORTS

Within 45 days of the end of each calendar quarter following the effective date of this ORDER, the SP must furnish to the DRD written progress reports detailing the form, manner, and results of any actions taken to secure compliance with this ORDER. All progress reports and other written responses to this ORDER must be reviewed and approved by the Board and be made a part of the Board minutes.

IV. LETTER TO INSURED DEPOSITORY INSTITUTIONS

At the same time the SP furnishes progress reports to the DRD, the SP must send a letter to the IDIs to which it is providing IT services accurately and completely describing the actions the SP has taken during the quarter to comply with this ORDER.

V. NOTICE TO PARENT HOLDING COMPANY

Within 30 days from the effective date of this ORDER, the Board must provide either a copy of this ORDER or an accurate and complete description of all material aspects of the ORDER to its parent company.

VI. OTHER ACTIONS

The provisions of this ORDER do not bar, estop, or otherwise prevent the FDIC or any other federal or state agency or department from taking any other action against the SP.

This ORDER is effective on the date of issuance and its provisions will remain effective and enforceable until a provision is modified, terminated, suspended, or set aside in writing by the FDIC. The provisions of this ORDER are binding upon the SP and any successors and

assigns thereof.

Issued Under Delegated Authority.

Dated: November 20, 2023

/s/

By: Marianne Hatheway
Deputy Regional Director
New York Region
Federal Deposit Insurance Corporation