

**UNITED STATES OF AMERICA
CONSUMER FINANCIAL PROTECTION BUREAU**

ADMINISTRATIVE PROCEEDING

File No. 2024-CFPB-0013

In the Matter of:

VyStar Credit Union

CONSENT ORDER

The Consumer Financial Protection Bureau (Bureau) has reviewed the banking activities of VyStar Credit Union (Respondent, as defined below) and has identified the following violations of law: Respondent engaged in unfair acts and practices in the provision of online and mobile banking services in violation of the Consumer Financial Protection Act of 2010 (CFPA), 12 U.S.C. §§ 5531, 5536(a)(1)(B). Under §§ 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563, 5565, the Bureau issues this Consent Order (Consent Order).

I.

Jurisdiction

1. The Bureau has jurisdiction over this matter under §§ 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563 and 5565.

II.

Stipulation

2. Respondent has executed a “Stipulation and Consent to the Issuance of a Consent Order,” dated October 15, 2024 (Stipulation), which is incorporated by reference and is accepted by the Bureau. By this Stipulation, Respondent has consented to the issuance of this Consent Order by the Bureau under §§ 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563, 5565, without admitting or denying any of the findings of fact or conclusions of law, except that Respondent admits the facts necessary to establish the Bureau’s jurisdiction over Respondent and the subject matter of this action.

III.

Definitions

3. The following definitions apply to this Consent Order:
 - a. “Affected Consumers” are members of Respondent’s credit union who used their credit union accounts for personal, family, or

household purposes and who incurred fees or costs, including but not limited to interest costs, as a result of the disruption in service of Respondent's virtual banking platform.

- b. "Board" means Respondent's duly-elected and acting Board of Directors.
- c. "Consumer Facing Banking System" means an electronic interface comprising software, hardware, or user-facing design provided by Respondent and used directly by Respondent's members to conduct banking activities, monitor accounts, or access banking related information.
- d. "Effective Date" means the date on which the Consent Order is entered on the administrative docket.
- e. "Enforcement Director" means the Assistant Director of the Office of Enforcement for the Consumer Financial Protection Bureau, or their delegate.
- f. "Key Vendor" means a vendor retained by Respondent for a Consumer Facing Banking Systems project that builds, modifies, designs, consults on, or maintains customized software, digital tools, or other information technology infrastructure.

- g. “Related Consumer Action” means a private action by or on behalf of one or more consumers or an enforcement action by another governmental agency brought against Respondent based on substantially the same facts as described in Section IV of this Consent Order.
- h. “Respondent” means VyStar Credit Union, and its successors and assigns.
- i. “Respondent’s Executives” means Respondent’s Chief Executive Officer, President, Executive Vice President, Chief Operating Officer, Chief Information Officer, Chief Technology Officer, and Chief Retail Officer, or their equivalents.
- j. “Supervision Director” means the Assistant Director of the Office of Supervision for the Consumer Financial Protection Bureau, or their delegate.

IV.

Bureau Findings and Conclusions

The Bureau finds the following:

- 4. Respondent is a Florida state-chartered credit union headquartered in Jacksonville, Florida. As of July 31, 2024, Respondent had approximately \$14.72 billion in total assets.

5. Respondent is an insured credit union with assets greater than \$10,000,000,000 within the meaning of 12 U.S.C. § 5515(a).
6. Respondent engages in deposit-taking activities, transmits or exchanges funds, or otherwise acts as a custodian of funds for use by or on behalf of consumers primarily for personal, family, or household purposes, and therefore offers a consumer financial product or service, 12 U.S.C. § 5481(15)(A)(iv). Thus, Respondent is a “covered person” under 12 U.S.C. § 5481(6).
7. As of 2022, Respondent had 850,000 members with deposit accounts at the credit union.
8. Respondent maintains online and mobile banking services through a virtual banking platform that provides members, among other things, the ability to (i) access their account balances, (ii) transfer funds between their accounts, such as between their checking and savings accounts, (iii) make credit card and loan payments, (iv) deposit checks remotely, and (v) set up recurring or one-time payments for third party bills. Most of Respondent’s members have signed up for the virtual banking platform, and in any given month, somewhat more than half of Respondent’s members use the virtual banking platform to do all or part of their banking.

9. Respondent's virtual banking platform can be accessed by its members using a web-based interface on Respondent's website, and through a mobile application interface on smartphones.
10. In May 2022, Respondent attempted to launch a new virtual banking platform. The conversion to the new virtual banking platform involved disabling the prior virtual banking platform (the "Precursor Platform") and replacing it with new systems designed and built by Respondent and the vendor it selected for the project (the "Vendor").
11. Under Respondent's original plan, the conversion to the new virtual banking platform would have required only a brief interruption of services for its members, from May 13 to May 15, 2022, as the Precursor Platform was taken offline, and the new platform was made available to Respondent's members.
12. However, shortly after the new virtual banking platform was made available to members, it became unstable, intermittently losing functionality and abandoning processes initiated by members, such as attempts to log into their accounts. These performance issues required Respondent to take the platform offline on May 17, 2022.
13. On May 23, 2022, Respondent relaunched a limited version of the web-based interface which omitted significant features previously utilized by

Respondent's members. The limited version did not provide members (i) access to their account statements, (ii) the ability to make internal transfers between accounts, (iii) credit card and loan payment functions, (vi) the ability to set up recurring payments, or (v) access to full transaction histories.

14. In order to protect the stability of the limited version of the virtual banking platform web-based interface, Respondent regulated member access to the system through the use of "virtual waiting rooms." At certain points these rooms contained thousands of members, and members reported extensive wait times, with at least one person complaining to the Bureau of a wait time in excess of four hours.
15. The failure of the virtual banking platform led to a massive increase in members contacting Respondent's call center, beyond its capacity to meet the demand. In the week commencing on May 15, calls increased nearly 250%, with a 33% drop rate. The high drop rates persisted for months, ranging between 31 and 44%.
16. Members also reported long lines and wait times at Respondent's branches, and members who lived outside of Respondent's service area had no access to a branch.

17. The other banking options available to members during the virtual banking platform outage lacked the features and functions of the Precursor Platform. Respondent's Magic*Touch system, an automated telephonic banking service, offered limited services and was available only to members who had previously set up access through a branch or the call center. Likewise, Respondent's ATMs could not be used to make payments to third parties, and members could not use the "surcharge-free" ATMs in Respondent's extended network to deposit checks, or use other third-party ATMs to deposit checks, without incurring a fee.
18. In the weeks and months following the failure, Respondent slowly phased features back into the new virtual banking platform. Full functionality, i.e., a return of all the features available in the Precursor Platform, was not restored until December 2022.
19. The mobile application interface suffered a greater disruption. Respondent's mobile application interface was completely unavailable for a month after the initial failure. Like the web-based interface, the initial version of the relaunched mobile application interface lacked key banking features, which were slowly reintroduced over the course of several months.
20. During the virtual banking platform outage and period of limited functionality, Respondent's members' ability to effectively manage their

finances was meaningfully diminished. For a sustained period, members could less readily (i) access their account balances, (ii) transfer funds between accounts, and (iii) make payments on credit card balances and loans on VyStar accounts. Some members' previously scheduled recurring payments were delayed or even deleted.

21. These issues caused Respondent's members to risk incurring or incur, among other fees, non-sufficient funds (NSF) fees, overdraft fees, late fees, bounced check fees, and fees for alternate payment methods, such as wire transfer fees. Some members also incurred interest charges for late payments that resulted from the virtual banking platform failure. Impacted members were also at increased risk of harm to their credit reports and scores from reporting related to late payments on credit cards, loans, and other bills.
22. Likewise, because members could not determine their actual account balances using their computers or mobile devices—whether funds had been deposited, transactions had cleared, or fees had been incurred—their ability to prioritize payment decisions was impaired.

The Virtual Banking Platform's Collapse was Caused by Respondent's Failure to Establish Reasonable Management and Governance Processes and Procedures

23. The virtual banking platform outage and sustained period of limited functionality were the result of Respondent's management and governance

failures and its assumption of excessive risk throughout the conversion project. Industry standard risk management engineering practices for such a project were ignored in favor of speed and cutting costs. The resulting harms to consumers were predictable and avoidable.

24. Numerous decisions made by Respondent led directly to the failure to maintain key banking services for consumers, including the decisions not to institute project management guardrails, to adopt a rushed, aggressive project timeline, and to ignore red flags about problems with the new platform. The impact of these decisions and actions was magnified by Respondent's selection of the Vendor, who was inexperienced in projects with the complexity of this conversion.
25. Respondent's lack of project management guardrails, and lack of sufficient governance, allowed Respondent to select the Vendor as the primary vendor for the virtual banking platform project outside of its normal procurement process. After initially selecting a different e-banking platform vendor through Respondent's formal request for proposals process, in March 2021, Respondent changed course and selected the Vendor without initiating a new request for proposals process or conducting the normal due diligence that such a process would entail. Project managers were able to ignore parts of the requests for proposals and due diligence processes because Respondent

failed to have governance structures in place that would detect and correct these deviations. The modified requests for proposals process resulted in material deficiencies in the evaluation of the Vendor; for example, the review of the proof of concept submitted by the Vendor, a miniature version of a key piece of the virtual banking platform, failed to provide a meaningful examination of the design and development challenges of the project.

26. Respondent selected the Vendor without considering key factors such as the fact that the Vendor's product offerings were not compatible with Respondent's core transaction processing system without implementing more extensive customized software than would have been required with a different vendor. This lack of compatibility required the Vendor to design and implement custom integration code to link its front-end system with Respondent's core banking processing system. The Vendor had never performed a conversion that required it to integrate its virtual banking products with an existing core processing system that originated from a different vendor in this way. Likewise, Respondent selected the Vendor despite knowing it lacked experience performing banking system conversions this complex.
27. Concurrent with its hiring of the Vendor, Respondent made a \$20 million investment in the Vendor, in the hope that the virtual banking platform

project would demonstrate the Vendor's services to other financial institutions and lead to the creation of products and services that Respondent and the Vendor could sell to others. The contract with the Vendor included a 28% discount on the five-year vendor agreement associated with the platform conversion.

28. Respondent did not take actions or incorporate plans into the conversion project taking into account the challenges incumbent in selecting the Vendor and its technology. For example, Respondent retained its original timeline for developing, testing, and releasing the new virtual banking platform.
29. In addition to not accounting for the challenges associated with selecting the new Vendor and the project's complexity, Respondent failed to take steps expected in any major project like this one. For example, Respondent failed to adopt numerous industry standard governance structures, including a formal statement of work governing the technical aspects of the platforms, a single centralized scope of project document, risk-and-issue management plans and logs, or enforceable benchmarks and completion standards for the Vendor.
30. During this critical phase of the conversion project—when the Respondent transitioned to the Vendor as its primary project vendor and set the development schedule—Respondent lacked a Chief Information Officer. As

a result, the project's most senior leadership made critical decisions that required input from personnel with a technical background without such a person at the highest ranks.

31. Respondent also performed insufficient testing of the virtual banking platform prior to and during conversion. For example, Respondent failed to sufficiently test the custom integration code that linked the Vendor's systems to its core banking systems. Likewise, Respondent never performed testing that would simulate expected transaction load levels. As a result, the platforms were not assessed prior to release in a manner appropriate for their complexity and criticality.
32. The testing that was performed by Respondent, up to the time of the release, consistently showed significant, material issues with the virtual banking platform's quality. Despite these issues, Respondent failed to adequately manage conversion risks, including by not exploring the feasibility of lower-risk conversion options, such as "piloting" the virtual banking platform with small, increasing, numbers of its members, and not developing contingencies that would have allowed reversion to the Precursor Platform, if necessary.
33. During the project, to keep to its project timelines, Respondent became increasingly willing to accept the persistence of critical bugs and lower levels of functionality in the new virtual banking platform. This occurred

simultaneously with an increasing prevalence of new bugs within the platform as the project got closer to release. Rather than address these issues before the conversion, Respondent chose to rely on what is commonly referred to as a “fast follow” approach. This decision shifted the timeframe for fixing bugs and improving functionality to after the new platform was released and serving as the only available system for Respondent’s members.

34. Shortly before the May 13, 2022 release, Respondent’s management leading the project downgraded the classification of at least 135 defects identified in the virtual banking platform that were initially classified as critical. This change in status meant that the identified defects did not have to be addressed prior to the initiation of the conversion. When employees from Respondent’s Information Technology Audit group inquired about the downgrading of these defects, Respondent’s management leading the project told them that these decisions had been communicated to senior management. This representation was false.
35. Respondent’s tolerance of defects, bugs, lower standards of functionality, and inadequate testing was at odds with Respondent’s Quality Assurance team, which was responsible for testing the virtual banking platform. The head of the Quality Assurance team refused to sign off on the virtual

banking platform because of these issues, and the downgrading of the 135 defects, in particular. Despite the Quality Assurance team's objections, Respondent went forward with the release of the new virtual banking platform, dismissing the Quality Assurance team's concerns as simply a product of their risk-averse mentality.

36. Respondent also ignored feedback from the project development team that the virtual banking platform was not ready for release, creating significant reputational risk and raising the real possibility that the outcome would lead to negative publicity. Respondent likewise failed to assess whether there was a broad consensus across the development team that the platform was ready for launch in the months leading up to release. Had they done so, they may have discovered that it was well known among the development team that the platform was not ready for general use by Respondent's members.
37. Respondent chose to utilize a conversion process that irrevocably disabled the Precursor Platform when the new virtual banking platform was brought online. This left Respondent and its members without a backup in the event that the new platform failed to perform. This decision was made despite the Vendor having never participated in a similar complex banking systems project, the reliance on a "fast follow" approach which left the correction of

- known issues until after release, management's downgrading of critical defects, and the decision to maintain an unrealistic completion timeframe.
38. Additionally, Respondent failed to establish, memorialize, or follow objective standards to determine the virtual banking platform's implementation readiness. Because of this, the final decision to start the conversion was influenced by various subjective factors and considerations outside of the platform's ability to perform its intended functions.
39. Respondent made the decision that the new virtual banking platform had to be in place by May 2022 because waiting would have required it to convert to the Precursor Platform's updated banking platform and continue to pay \$1 million for each month it used the Precursor Platform. Because of this required upgrade to the Precursor Platform, Respondent would have been required to keep the Precursor Platform until at least August of 2022, and Respondent would not have been able to convert to the new virtual banking platform with Vendor until after that time. As a result, Respondent rushed the release of the virtual banking platform.
40. Throughout the development, implementation, and release of the virtual banking platform, Respondent, despite the significance of the platform for its operations, failed to maintain reasonable management and governance procedures to ensure that the Board and most senior executives were aware

of the seriousness of the issues encountered during the project, and that the project was more complex and carried more risk than an ordinary virtual banking platform conversion.

41. Respondent's prior implementation of a new virtual banking platform, in 2016, also resulted in a service disruption, though of a smaller scale. That disruption similarly resulted from the assumption of excessive risk, in particular a lack of adequate contingency planning. Therefore, significant problems with the new virtual banking platform were foreseeable and, if Respondent had established reasonable management and governance processes and procedures, avoidable.
42. Respondent's acts and practices described herein resulted in Affected Consumers being assessed fees and additional interest costs due to missed payments. Respondent reimbursed or proactively waived more than \$2.5 million in fees that it imposed or would have imposed, and it reimbursed its members for some third-party fees and additional interest costs.
43. Section 1036(a)(1)(B) of the CFPA prohibits "unfair, deceptive, or abusive" acts or practices. 12 U.S.C. § 5536(a)(1)(B).
44. A practice is unfair if it causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by the consumers, and such

substantial injury is not outweighed by countervailing benefits to consumers or competition. 12 U.S.C. §§ 5531(c).

45. The virtual banking platform outage and limited functionality resulted in substantial financial and non-financial harm to consumers, including fees, costs, and inconvenience. Respondent's failure to establish reasonable management and governance processes or procedures to prevent consumers' loss of access to and control over their accounts, including its lack of project management guardrails, selection of an untested vendor, rushed timing, and ignoring of red flags that problems existed, caused or was likely to cause consumers substantial injury.
46. Consumers could not reasonably avoid the injury caused by the virtual banking platform outage and limited functionality because Respondent alone controlled the development and implementation of the system. Respondent did not provide consumers with alternatives that could provide similar services.
47. The virtual banking platform outage and limited functionality did not provide countervailing benefits to consumers or competition. Consumers accrued no benefit from the virtual banking platform failure, and Respondent does not suffer any competitive disadvantage by having to provide its members with a usable virtual banking platform.

48. Therefore, as described in Paragraphs 4-47, Respondent engaged in unfair acts and practices in the provision of virtual banking services in violation of the CFPA, 12 U.S.C. §§ 5531; 5536(a)(1)(B).

V.

Conduct Provisions

Prohibited Conduct

IT IS ORDERED, under §§ 1053 and 1055 of the CFPA, that:

49. Respondent and its officers, agents, servants, employees, and attorneys, and all other persons in active concert or participation with them who receive actual notice of this Consent Order, whether acting directly or indirectly, in connection with changes, upgrades, maintenance, modernization, overhauls, or replacements of its Consumer Facing Banking Systems may not violate sections 1031 and 1036 of the CFPA, 12 U.S.C. §§ 5531 and 5536, and are prohibited from hiring, retaining, or otherwise entering into any services or purchase contract with any Key Vendor outside of Respondent's procurement and due diligence policies and procedures.

Affirmative Requirements

IT IS ORDERED, under §§ 1053 and 1055 of the CFPA, that:

50. Respondent must take the following affirmative actions:

- a. Establish and maintain a committee, or use an existing committee, (the “Committee”), as follows:
 - i. The Committee must:
 - (1) Assess potential risk to members arising from ongoing or recurring technology issues;
 - (2) Ensure that the selection of all Key Vendors is in compliance with Respondent’s procurement and due diligence policies and procedures;
 - (3) Direct the development, implementation, release, and maintenance of all Consumer Facing Banking Systems; and
 - (4) Direct the implementation, maintenance, and enforcement of any new or revised policies required by Subparagraph 50(c).
 - ii. The Committee must solicit and review regular reports from the officers and employees best positioned to assess and address member risk and compliance risk related to Respondent’s Consumer Facing Banking Systems, including the Chief Risk Officer, Chief Compliance Officer, Chief Technology Officer, and the lead for member experience, or their equivalents that:
 - (1) Assess the performance of each Consumer Facing Banking System;

- (2) Identify and prioritize upgrades and replacements for all Consumer Facing Banking Systems; and
 - (3) Receive, review, or respond to member complaints.
- iii. The Committee must timely provide Respondent's Chief Executive Officer with:
 - (1) Proposed solutions for any risks to members identified by the Committee;
 - (2) Proposed solutions to any outstanding technology issues related to any Consumer Facing Banking Systems; and
 - (3) Recommendations for additional technology resources for Consumer Facing Banking Systems.
- iv. The Committee must make the final recommendation to the Board regarding the ultimate conversion of any Consumer Facing Banking System replacements, overhauls, or modernization plans. The Board will be responsible for final sign off on any such conversions, unless it has delegated such final sign off to the Committee.
- v. The Committee must comprise, at a minimum, the Chief Executive Officer, Chief Operating Officer, Chief Legal Officer, Chief Information Officer, and Chief Financial Officer.

- vi. The Committee must provide regular reports to the Board that include its assessments of potential member risk from Consumer Facing Banking Systems.
- b. Respondent must establish, implement, and maintain contingency plans for Consumer Facing Banking Systems to minimize the impact of any failures on members, as follows:
 - i. Respondent must establish, implement, and maintain software development lifecycle policies that require any proposed release or conversion of a Consumer Facing Banking System that would replace, overhaul, or modernize an existing legacy system or functionality thereof (“Covered Release”) adequately account for the possibility of failure in connection with the Covered Release.
 - (1) This policy must include, at a minimum, a requirement that all Covered Releases include appropriate contingencies designed to minimize or avoid unplanned disruption of members’ access to their accounts or transactions tied to their accounts held by Respondents.
 - a. As appropriate to the Covered Release at issue, these contingencies would include:
 - i. disaster-recovery or other failover options; or

- ii. maintenance of the option of reverting to legacy systems in the event the Covered Release encountered a technical failure that would materially impact members' access to their accounts or transactions tied to their accounts held by Respondent.
- ii. Respondent must establish, implement, and maintain a customer service management plan that allocates sufficient resources to Respondent's customer service call center, branches, information technology infrastructure, online banking platform, and mobile banking platform, as applicable, to accommodate significant member use increases during and after Consumer Facing Banking System releases.
- c. Respondent must establish, implement, maintain, and enforce written policies and procedures that meet or exceed industry standards for the following:
 - i. Real-world load-requirement testing, prior to and continually after release, of Consumer Facing Banking Systems;

- ii. Final evaluation and determination to release decisions for Consumer Facing Banking Systems, also known as “Go/no-go decisions”; and
- iii. Project management for changes, upgrades, maintenance, modernization, or replacements of Consumer Facing Banking Systems, including but not limited to policies and procedures for:
 - (1) Project estimates;
 - (2) Scoping-of-project document creation and utilization; and
 - (3) Establishment and enforcement of benchmarks and completion standards for vendors and internal development teams.
- d. Respondent must conduct an audit of the reimbursement requests submitted by Affected Consumers pursuant to Respondent’s 2022 refund process (Refund Audit) to verify that all fees and costs resulting from the virtual banking platform outage and period of limited functionality, including but not limited to interest costs, were refunded to members who submitted requests. The Refund Audit will verify (i) that all monetary relief requested was reimbursed consistent with the original parameters of the refund process, and (ii) whether there are Affected Consumers who

may have been eligible to request interest but failed to do so, in which case VyStar will reimburse the amount of that interest.

- e. Respondent must reimburse members who submitted requests all previously uncompensated fees and costs identified by the Refund Audit.

VI.

Compliance Plan

IT IS FURTHER ORDERED that:

- 51. Within 60 days of the Effective Date, Respondent must create and implement a comprehensive compliance plan designed to ensure that Respondent's policies, procedures, and practices relating to changes, upgrades, maintenance, modernizations, overhauls, and replacements for its Consumer Facing Banking Systems comply with all applicable laws that the Bureau enforces, including Federal consumer financial laws, and the terms of this Consent Order (Compliance Plan). The Compliance Plan must include, at a minimum:
 - a. Detailed steps for addressing each action required by this Consent Order;
 - b. A mechanism to ensure that the Board is kept apprised of the status of compliance actions; and

- c. Specific timeframes and deadlines for implementation of the steps described above.

Respondent will provide the Compliance Plan to the Bureau upon request.

VII.

Role of the Board and Executives

IT IS FURTHER ORDERED that:

52. Respondent's Board has the ultimate responsibility for ensuring that Respondent complies with this Consent Order.
53. Respondent's Executives and Respondent's Board must review all plans and reports required by this Consent Order, and any submissions to the Bureau prior to such submission.
54. One year after the Effective Date, Respondent must submit to the Supervision Director an accurate written compliance progress report (Compliance Report) that has been approved by the Board and Respondent's Executives, the accuracy of which is sworn to under penalty of perjury, and which, at a minimum:
 - a. Describes the steps that Respondent's Executives have taken to reasonably assess whether Respondent is complying with the Compliance Plan and the Redress Plan, and each applicable paragraph and subparagraph of the Consent Order;

- b. Describes in detail whether and how Respondent has complied with the Compliance Plan and the Redress Plan, and each applicable paragraph and subparagraph of the Consent Order, including the manner of verification of such compliance and any corrective actions taken to remedy potential non-compliance with the applicable requirement, paragraph, or subparagraph; and
 - c. Attaches a copy of each Order Acknowledgment obtained under Section XV unless previously submitted to the Bureau.
55. Respondent's Board and Respondent's Executives must:
- a. Authorize whatever actions are necessary for Respondent to assess whether Respondent is complying with the Compliance Plan and the Redress Plan, and each applicable paragraph and subparagraph of the Consent Order;
 - b. Authorize whatever actions, including corrective actions, are necessary for Respondent to fully comply with the Compliance Plan and the Redress Plan, and each applicable paragraph and subparagraph of the Consent Order; and
 - c. Require timely reporting by management to Respondent's Board and Respondent's Executives on the status of compliance obligations.

MONETARY PROVISIONS

VIII.

Order to Pay Redress

IT IS FURTHER ORDERED that:

56. Within 45 days of the Effective Date, Respondent must submit to the Enforcement Director for review and non-objection a comprehensive written plan for identifying and providing redress to any Affected Consumer who has not already received full redress for financial harm caused by the virtual banking platform outage, consistent with this Consent Order (Redress Plan). The Enforcement Director will have the discretion to make a determination of non-objection to the Redress Plan or direct Respondent to revise it. If the Enforcement Director directs Respondent to revise the Redress Plan, Respondent must revise and resubmit the Redress Plan to the Enforcement Director within 15 days. After receiving notification that the Enforcement Director has made a determination of non-objection to the Redress Plan, Respondent must implement and adhere to the steps, recommendations, deadlines, and timeframes outlined in the Redress Plan.
57. The Redress Plan must:
 - a. Describe Respondent's methodology used to identify all Affected Consumers and determine the amount of redress that Respondent will

provide or has provided to each Affected Consumer, including the methodology used in the Refund Audit, for financial harm incurred as a result of the virtual banking platform outage; to wit, fees and costs, including but not limited to interest costs, incurred as a result of the disruption in service of Respondent's virtual banking platform;

- b. Provide for reimbursement of any such third-party fees and costs to all such Affected Consumers for the conduct described in Section IV of this Consent Order;
- c. Describe in full the steps Respondent will undertake to allow all Affected Consumers to seek reimbursement for third-party fees and costs incurred as a result of the virtual banking platform outage;
- d. Describe in full the steps Respondent will take to notify such Affected Consumers that they may submit reimbursement requests for third-party fees and costs incurred because of the virtual banking platform outage and period of limited functionality;
- e. Define the period of the reimbursement process, which shall remain open for no less than 6 months after the last date Respondent sends notices of such process to consumers;
- f. Specify that the criteria for approving reimbursement requests from Affected Consumers shall not require consumers to submit anything

- more than (i) a statement from the consumer of the third-party fees and costs incurred as result of the virtual banking platform outage and (ii) proof of payment of such fees and costs;
- g. Provide a copy of all email and written communications, website postings, texts messages, or any other means Respondent will use to inform consumers of their ability to submit reimbursement requests;
 - h. Provide for a dedicated email address and telephone number that consumers may use in the event they have reimbursement related questions;
 - i. Include the form of the communication (Redress Notice) and any envelope to be sent notifying Affected Consumers who are entitled to redress of their right to redress; the Redress Notice must include a statement that the payment is made in accordance with the terms of this Consent Order; Respondent must not include in any envelope containing a Redress Notice any materials other than the approved Redress Notice, unless Respondent has written confirmation from the Enforcement Director that the Bureau does not object to the inclusion of such additional materials;
 - j. Provide that redress will be paid to Affected Consumers through direct deposit, which will not be subject to offsets, and where

direct deposits are impracticable, redress will be paid by check to the Affected Consumer;

k. Describe the process for providing redress to Affected Consumers, and must include the following requirements:

- i. Respondent must make a direct deposit or mail a redress check and the applicable Redress Notice to every Affected Consumer, or their authorized representative, entitled to redress;
- ii. Prior to sending redress checks and Redress Notices, Respondent must make reasonable attempts to obtain a current address for every Affected Consumer entitled to redress using, at a minimum, the National Change of Address System (NCAS). If no updated address is provided by NCAS, the Respondent may mail the Redress Notice and redress check to the consumer's last known mailing address;
- iii. Respondent must send any redress check by United States Postal Service first-class mail, address correction service requested, to the most recent address for every Affected Consumer entitled to redress refunded by check;
- iv. If a redress check is returned to Respondent as undeliverable,

Respondent must make additional reasonable attempts to contact the Affected Consumer and obtain a current address using a commercially available database other than the NCAS or by skip-tracing, emailing, or contacting the Affected Consumer at the individual's last known email address or phone number. Respondent must identify Affected Consumers with undelivered checks to the Bureau within 30 days of the returned mail. Respondent must promptly re-mail all returned redress checks and the Redress Notice to the current addresses, if any, obtained through such reasonable attempts or through Bureau-provided addresses;

v. Respondent must turn over any redress amount remaining unclaimed after 180 days from the date the check was mailed or re-mailed, whichever is later, to the Bureau as set forth in Paragraph 59;

- l. Set forth all procedures, deadlines, and time frames for completing each step of the Redress Plan, consistent with the terms of this Consent Order; and
- m. Identify Respondent's officers, agents, servants, employees, and attorneys responsible for executing administration of the Redress

Plan.

58. Within 30 days of completing the Redress Plan, Respondent must submit to the Bureau a Redress Report detailing the number of consumers who received redress, the total amount of redress paid to those consumers, and any remainder of funds to be wired to the Bureau pursuant to Paragraph 59.
59. Within 30 days of the completion of the Redress Plan, Respondent must pay to the Bureau, by wire transfer to the Bureau or the Bureau's agent, and according to the Bureau's wiring instructions, the amount of redress checks that were not cashed by Affected Consumers.
60. The Bureau may use these funds to pay additional redress to Affected Consumers. If the Bureau determines, in its sole discretion, that additional redress is wholly or partially impracticable or otherwise inappropriate, or if funds remain after the additional redress is completed, the Bureau will deposit any remaining funds in the U.S. Treasury. Respondent will have no right to challenge any actions that the Bureau or its representatives may take under this Section.
61. Respondent may not condition the payment of any redress to any Affected Consumer under this Consent Order on that Affected Consumer waiving any right.

IX.

Order to Pay Civil Money Penalty

IT IS FURTHER ORDERED that:

62. Under § 1055(c) of the CFPA, 12 U.S.C. § 5565(c), by reason of the violations of law described in Section IV of this Consent Order, Respondent must pay a civil money penalty of \$1,500,000 to the Bureau.
63. Within 10 days of the Effective Date, Respondent must pay the civil money penalty by wire transfer to the Bureau or to the Bureau's agent in compliance with the Bureau's wiring instructions.
64. The civil money penalty paid under this Consent Order will be deposited in the Civil Penalty Fund of the Bureau as required by § 1017(d) of the CFPA, 12 U.S.C. § 5497(d).
65. Respondent, for all purposes, must treat the civil money penalty paid under this Consent Order as a penalty paid to the government. Regardless of how the Bureau ultimately uses those funds, Respondent may not:
 - a. Claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for any civil money penalty paid under this Consent Order; or
 - b. Seek or accept, directly or indirectly, reimbursement or indemnification from any source, including but not limited to payment

made under any insurance policy, with regard to any civil money penalty paid under this Consent Order.

66. To preserve the deterrent effect of the civil money penalty in any Related Consumer Action, Respondent may not argue that Respondent is entitled to, nor may Respondent benefit by, any offset or reduction of any compensatory monetary remedies imposed in the Related Consumer Action because of the civil money penalty paid in this action or because of any payment that the Bureau makes from the Civil Penalty Fund. If the court in any Related Consumer Action offsets or otherwise reduces the amount of compensatory monetary remedies imposed against Respondent based on the civil money penalty paid in this action or based on any payment that the Bureau makes from the Civil Penalty Fund, Respondent must, within 30 days after entry of a final order granting such offset or reduction, notify the Bureau, and pay the amount of the offset or reduction to the U.S. Treasury. Such a payment will not be considered an additional civil money penalty and will not change the amount of the civil money penalty imposed in this action.

X.

Additional Monetary Provisions

IT IS FURTHER ORDERED that:

67. In the event of any default on Respondent's obligations to make payment under this Consent Order, interest, computed under 28 U.S.C. § 1961, as amended, will accrue on any outstanding amounts not paid from the date of default to the date of payment, and will immediately become due and payable.
68. Respondent must relinquish all dominion, control, and title to the funds paid to the fullest extent permitted by law and no part of the funds may be returned to Respondent.
69. Respondent acknowledges that its Employer Identification Number, which Respondent previously submitted to the Bureau, may be used for collecting and reporting on any delinquent amount arising out of this Consent Order, in accordance with 31 U.S.C. § 7701.
70. Within 30 days of the entry of a final judgment, consent order, or settlement in a Related Consumer Action, Respondent must notify the Supervision Director of the final judgment, consent order, or settlement in writing. That notification must indicate the amount of redress, if any, that Respondent paid

or is required to pay to consumers and describe the consumers or classes of consumers to whom that redress has been or will be paid.

COMPLIANCE PROVISIONS

XI.

Reporting Requirements

IT IS FURTHER ORDERED that:

71. Respondent must notify the Bureau of any development that may affect compliance obligations arising under this Consent Order, including but not limited to a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this Consent Order; the filing of any bankruptcy or insolvency proceeding by or against Respondent; or a change in Respondent's name or address. Respondent must provide this notice, if practicable, at least 30 days before the development, but in any case no later than 14 days after the development.
72. Within 7 days of the Effective Date, Respondent must:
 - a. designate at least one telephone number and email, physical, and postal addresses as points of contact that the Bureau may use to communicate with Respondent;

- b. designate at least one telephone number and email, physical, and postal addresses as points of contact for consumers with inquiries related to consumer relief under the Consent Order;
 - c. identify all businesses for which Respondent is the majority owner, or that Respondent directly or indirectly controls, by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; and
 - d. describe the activities of each such business, including the products and services offered, and the means of advertising, marketing, and sales.
73. Respondent must report any change in the information required to be submitted under Paragraph 71 at least 30 days before the change or as soon as practicable after the learning about the change, whichever is sooner.

XII.

Order Distribution and Acknowledgment

IT IS FURTHER ORDERED that:

74. Within 7 days of the Effective Date, Respondent must submit to the Supervision Director an acknowledgment of receipt of this Consent Order, sworn under penalty of perjury.

75. Within 30 days of the Effective Date, Respondent must deliver a copy of this Consent Order to each of its Board members and executive officers, as well as to any managers, employees, service providers, or other agents and representatives who have responsibilities related to the subject matter of the Consent Order.
76. For 5 years from the Effective Date, Respondent must deliver a copy of this Consent Order to any business entity resulting from any change in structure referred to in Section XI, any future board members and executive officers, as well as to any managers, employees, service providers, or other agents and representatives who will have responsibilities related to the subject matter of the Consent Order before they assume their responsibilities.
77. Respondent must secure a signed and dated statement acknowledging receipt of a copy of this Consent Order, within 30 days of delivery, from all persons receiving a copy of this Consent Order under this Section.
78. Ninety days from the Effective Date, Respondent must submit to the Bureau a list of all persons and their titles to whom this Consent Order has been delivered under the Section of this Consent Order titled “Order Distribution and Acknowledgment” and a copy of all signed and dated statements acknowledging receipt of this Consent Order under Paragraph 75.

XIII.

Recordkeeping

IT IS FURTHER ORDERED that:

79. Respondent must create and retain the following business records:
- a. All documents and records necessary to demonstrate full compliance with the Compliance Plan and each provision of this Consent Order, including all submissions to the Bureau;
 - b. All documents and records pertaining to the Redress Plan;
 - c. Meeting minutes of the Board, its committees, and the Committee described in Paragraph 50, regarding Respondent's compliance with this Consent Order and the Compliance Plan, with sufficient detail to document the substance of all matters discussed;
 - d. All consumer complaints relating to any changes, upgrades, maintenance, or replacements for Consumer Facing Banking Systems (including but not limited to requests for refunds) and any responses to those complaints or requests;
 - e. Documents reflecting all unique communications or representations to consumers relating to any changes, upgrades, maintenance, or replacements for Consumer Facing Banking Systems;
 - f. Copies of any contracts with any Key Vendors for services relating to

any changes, upgrades, maintenance, or replacements for Consumer Facing Banking Systems;

- g. Records showing, for each Key Vendor providing services related to online or mobile banking, the name of a point of contact, and that person's telephone number, email, physical, and postal address, job title or position, dates of service, and, if applicable, the reason for termination.
80. All documents and records must be maintained in their original electronic format. Data should be centralized, and maintained in such a way that access, retrieval, auditing, and production are not hindered.
81. Respondent must make the documents identified in Paragraph 79 available to the Bureau upon the Bureau's request.

XIV.

Notices

IT IS FURTHER ORDERED that:

82. Unless otherwise directed in writing by the Bureau, Respondent must provide all submissions, requests, communications, or other documents relating to this Consent Order in writing, with the subject line, "*In re* VyStar Credit Union, File No. 2024-CFPB-0013," and send them to the following email: Enforcement_Compliance@cfpb.gov addressed as follows:

ATTN: Supervision Director
Consumer Financial Protection Bureau
Office of Supervision

ATTN: Enforcement Director
Consumer Financial Protection Bureau
Office of Enforcement

XV.

Cooperation with the Bureau

IT IS FURTHER ORDERED that:

83. Respondent must cooperate fully to help the Bureau determine the identity and location of, and the amount of injury sustained by, each Affected Consumer. Respondent must provide such information in its or its agents' possession or control within 14 days of receiving a written request from the Bureau.

XVI.

Compliance Monitoring

IT IS FURTHER ORDERED that:

84. Within 14 days of receipt of a written request from the Bureau, Respondent must submit additional Compliance Reports or other requested information, which must be made under penalty of perjury; provide sworn testimony; or produce documents.

85. For purposes of this Section, the Bureau may communicate directly with Respondent, unless Respondent retains counsel related to these communications.
86. Respondent must permit Bureau representatives to interview any employee or other person affiliated with Respondent who has agreed to such an interview regarding: (a) this matter; (b) anything related to or associated with the conduct described in Section IV; or (c) compliance with the Consent Order. The person interviewed may have counsel present.
87. Nothing in this Consent Order will limit the Bureau's lawful use of civil investigative demands under 12 C.F.R. § 1080.6 or other compulsory process.

XVII.

Modifications to Non-Material Requirements

IT IS FURTHER ORDERED that:

88. Respondent may seek a modification to non-material requirements of this Consent Order (*e.g.*, reasonable extensions of time and changes to reporting requirements) by submitting a written request to the Supervision Director.
89. The Supervision Director may, in their discretion, modify any non-material requirements of this Consent Order (*e.g.*, reasonable extensions of time and changes to reporting requirements) if they determine good cause justifies the

modification. Any such modification by the Supervision Director must be in writing.

XVIII.

ADMINISTRATIVE PROVISIONS

IT IS FURTHER ORDERED that:

90. The provisions of this Consent Order do not bar, estop, or otherwise prevent the Bureau from taking any other action against Respondent, except as specified in Paragraph 91. Further, for the avoidance of doubt, the provisions of this Consent Order do not bar, estop, or otherwise prevent any other person or governmental agency from taking any action against Respondent.
91. The Bureau releases and discharges Respondent from all potential liability for law violations that the Bureau has or might have asserted based on the practices described in Section IV of this Consent Order, to the extent such practices occurred before the Effective Date and the Bureau knows about them as of the Effective Date. The Bureau may use the practices described in this Consent Order in future enforcement actions against Respondent and its affiliates, including, without limitation, to establish a pattern or practice of violations or the continuation of a pattern or practice of violations or to calculate the amount of any penalty. This release does not preclude or affect

any right of the Bureau to determine and ensure compliance with the Consent Order, or to seek penalties for any violations of the Consent Order.

92. This Consent Order is intended to be, and will be construed as, a final Consent Order issued under § 1053 of the CFPA, 12 U.S.C. § 5563, and expressly does not form, and may not be construed to form, a contract binding the Bureau or the United States.
93. This Consent Order will terminate on the later of 5 years from the Effective Date or 5 years from the most recent date that the Bureau initiates an action alleging any violation of the Consent Order by Respondent if such action is initiated within 5 years of the Effective Date. If such action is dismissed or the relevant adjudicative body rules that Respondent did not violate any provision of the Consent Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Consent Order will terminate as though the action had never been filed. The Consent Order will remain effective and enforceable until such time, except to the extent that any provisions of this Consent Order have been amended, suspended, waived, or terminated in writing by the Bureau or its designated agent.
94. Calculation of time limitations will run from the Effective Date and be based on calendar days, unless otherwise noted.

95. Should Respondent seek to transfer or assign all or part of its operations that are subject to this Consent Order, Respondent must, as a condition of sale, obtain the written agreement of the transferee or assignee to comply with all applicable provisions of this Consent Order.
96. The provisions of this Consent Order will be enforceable by the Bureau. For any violation of this Consent Order, the Bureau may impose the maximum amount of civil money penalties allowed under §1055(c) of the CFPA, 12 U.S.C. § 5565(c). In connection with any attempt by the Bureau to enforce this Consent Order in federal district court, the Bureau may serve Respondent wherever Respondent may be found and Respondent may not contest that court's personal jurisdiction over Respondent.
97. This Consent Order and the accompanying Stipulation contain the complete agreement between the parties. The parties have made no promises, representations, or warranties other than what is contained in this Consent Order and the accompanying Stipulation. This Consent Order and the accompanying Stipulation supersede any prior oral or written communications, discussions, or understandings.
98. Nothing in this Consent Order or the accompanying Stipulation may be construed as allowing Respondent, its Board, its Executives, officers, or employees to violate any law, rule, or regulation.

IT IS SO ORDERED, this 31st day of October, 2024.

Rohit Chopra

Rohit Chopra
Director
Consumer Financial Protection Bureau