Memo

To: RIHousing Board of Commissioners
From: Brett Pelletier, Chief Administrative Officer (Qualified Individual)
cc: RIHousing Executive Team
Date: December 30, 2025
Re: **FTC Safeguards Rule Compliance – 2026 Report to Board of Commissioners**

Introduction

As you are aware, in 2021 the Federal Trade Commission (FTC) amended its Safeguards Rule to expand compliance and enforcement and, on December 9, 2021, published the Final Rule in the Federal Register. The provisions of the Rule went into effect variously on January 10, 2022, and December 9, 2022. Under the Amended Rule, organizations such as RIHousing are required to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to our size and complexity, the nature and scope of our activities, and the sensitivity of any customer information at issue. As part of compliance with the Safeguards Rule, the designated Qualified Individual must report in writing, regularly and at least annually, to the Board of Commissioners. The report must include the following:

- The overall status of the information security program and our compliance with the Safeguards Rule; and

- Material matters related to our information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

This report outlines the current status of our organization's compliance with the FTC Safeguards Rule and our progress in implementing a Zero Trust security model. As an organization that handles consumer financial data, it is imperative that we not only adhere to regulatory requirements but also implement robust, forward-thinking, and proactive security strategies. Our approach to cybersecurity now includes Zero Trust principles, which align with the FTC Safeguards Rule's emphasis on the protection of sensitive customer information.

FTC Safeguards Rule Overview

The FTC Safeguards Rule, part of the Gramm-Leach-Bliley Act (GLBA), mandates that financial institutions establish appropriate measures to safeguard customer information. The rule requires organizations to develop, implement, and maintain an information security program that includes administrative, technical, and physical safeguards designed to ensure the confidentiality and integrity of consumer financial data.

Key aspects of the Safeguards Rule that apply to our organization include:

1. **Risk Assessment:** A comprehensive risk assessment must be conducted to identify potential threats and vulnerabilities.
2. **Employee Training**: Staff must be trained on information security policies and procedures.
3. **Access Control**: Access to consumer information must be restricted based on need-to-know principles.
4. **Incident Response**: Procedures for responding to and reporting security breaches must be in place.
5. **Oversight and Accountability**: Regular monitoring and evaluation of the security program's effectiveness.

Compliance with the FTC Safeguards Rule Using Zero Trust

To align with the FTC Safeguards Rule and enhance our security posture, we have adopted the Zero Trust model as our core framework. Below is a summary of how we have integrated the principles of Zero Trust with the requirements of the FTC Safeguards Rule:

1. **Risk Assessment and Continuous Monitoring**
   The Zero Trust model's emphasis on continuous monitoring complements the FTC's requirement for ongoing risk assessments. We utilize tools provided by multiple highly trusted security vendors that continuously monitor and log all network activity. We can promptly detect and respond to threats, ensuring compliance with the requirement for an ongoing assessment of potential risks to consumer data.
2. **Access Control and Least Privilege Access**
   Zero Trust's core principle of "never trust, always verify" aligns with the FTC Safeguards Rule's stipulation that access to consumer information must be based on strict need-to-know principles. We are planning to implement role-based access controls (RBAC) using Microsoft Entra ID IAM service to ensure that users are granted the least amount of access necessary to perform their job functions.
3. **Employee Training and Awareness**
   Under Zero Trust, employees are continually educated on cybersecurity risks and behaviors. Our training programs, aligned with FTC requirements, focus on ensuring that staff members understand the risks of phishing, social engineering, and unauthorized access, and know how to comply with security protocols in day-to-day operations.
4. **Incident Response and Micro-Segmentation**
   Zero Trust enables a more proactive response to potential security incidents by using micro-segmentation to limit access to sensitive information. This method isolates different parts of the network, reducing the scope of a potential breach and facilitating quicker identification and

mitigation of threats, in line with the FTC Safeguards Rule's requirements for breach detection and response.

5. **Data Encryption and Secure Communication**
   As per both the FTC Safeguards Rule and Zero Trust principles, we ensure that all sensitive consumer data is encrypted both in transit and at rest. This encryption prevents unauthorized access, even if an attacker compromises a user or device.

Current Status and Next Steps

We are currently in a strong strategic position with regard to compliance with the FTC Safeguards Rule, bolstered by our ongoing implementation of the Zero Trust security framework. Key progress includes:

1. **Completed** a comprehensive Ransomware Readiness risk assessment in accordance with the FTC Safeguards Rule, identifying key vulnerabilities and threats to sensitive consumer data.
2. **Implemented** multi-factor authentication for all accounts including external partners that access our data, enabling strict authentication and authorization protocols across all user access points.
3. **Enhanced** data protection measures through encryption, micro-segmentation, and secure communication channels.
4. **Trained** employees on security best practices, with a focus on social engineering and phishing defense. In 2025, RIHousing achieved 100% participation during our annual cybersecurity training.
5. **Developed and tested** our Incident Response Plan and playbook.

Next steps include:

1. **Ongoing Evaluation**: Continuously evaluate our risk assessment framework and update it as new threats emerge. We are looking to engage with a third-party security vendor to provide a comprehensive and realistic review of our risk.
2. **Expansion of Zero Trust**: Further implementation of Zero Trust practices, including more strict device network access controls and increased use of AI-driven threat detection systems.
3. **Periodic Audits**: Conduct regular audits of our information security program to ensure compliance and identify areas for improvement.

Conclusion

By aligning our information security practices with the FTC Safeguards Rule and embracing the Zero Trust model, we are taking a proactive approach to safeguard sensitive consumer data and ensure that our organization is well-positioned to meet both regulatory and security challenges. We will continue to monitor and improve our security posture in line with best practices, ensuring compliance and minimizing risk.