Name: **Ayela Israr Haqqani**

Reg: **2022130**

To effectively mitigate the risk associated with the vulnerability in the authentication system of the online banking platform, a comprehensive risk mitigation plan should be developed. This plan will focus on addressing the immediate risk and implementing preventive measures to enhance the security of the system. Below is a step-by-step risk mitigation plan:

**1. Immediate Response**

* **Incident Response Team Activation:**
  + Assemble a dedicated incident response team (IRT) to address the current vulnerability and assess the impact of any unauthorized access.
* **System Audit:**
  + Conduct a thorough audit of the authentication system to identify how the vulnerability was exploited and assess the extent of unauthorized access.
* **User Notification:**
  + Inform affected users of the breach promptly and advise them to change their passwords and enable account monitoring for suspicious activity.

**2. Patch and Remediation**

* **Vulnerability Fixes:**
  + Work with the development team to create patches that address the vulnerabilities in the MFA system, ensuring that all potential bypass methods are secured.
* **Enhanced Logging:**
  + Implement or improve logging mechanisms for authentication attempts to detect and respond to unauthorized access attempts in real time.

**3. Security Enhancement**

* **Review MFA Implementation:**
  + Assess the current MFA implementation and explore integrating stronger MFA methods (e.g., biometric authentication, hardware tokens).
* **Zero Trust Approach:**
  + Adopt a zero-trust security model where every access request is verified regardless of source, ensuring that each user request is authenticated and authorized.
* **Regular Security Training:**
  + Conduct regular security awareness training for employees to ensure they understand the importance of security protocols and recognize potential phishing attacks.

**4. Ongoing Monitoring and Risk Assessment**

* **Continuous Security Monitoring:**
  + Implement continuous monitoring tools to track user behavior and detect anomalies that may indicate unauthorized access.
* **Regular Vulnerability Assessments:**
  + Schedule regular vulnerability assessments and penetration testing to identify and remediate any new security weaknesses in the system.

**5. Customer Trust and Communication**

* **Public Disclosure:**
  + Be transparent with customers about the breach, remedial actions taken, and future measures to prevent such occurrences, to rebuild trust.
* **Offering Credit Monitoring:**
  + Consider offering affected users free credit monitoring or identity theft protection services for a defined period to alleviate concerns over potential fraud.
* **Engagement with Regulators:**
  + Keep communication lines open with regulatory bodies regarding the breach, exploring scenarios for potential penalties or required remedial actions.
* **Immediate (0-1 week):** Incident response, user notifications, patch development.
* **Short-term (1-4 weeks):** Enhanced MFA implementation, logging improvements, and employee training.
* **Ongoing (1-3 months):** Continuous monitoring, vulnerability assessments, and compliance reviews.

The aim of this risk mitigation plan is to address the immediate risks posed by the vulnerability while establishing a framework for ongoing security improvements in the online banking system. By adopting a proactive security posture and ensuring transparent communication with users, the bank can not only address current issues but also strengthen its defenses against future attacks.