

**Date:** [Date]

**To:** [Customer Name / Department Name]

**Subject:** Urgent: Mobile Banking Security Vulnerability Advisory

Dear [Name],

This letter serves as a formal advisory regarding a newly identified security vulnerability affecting our mobile banking platform. Our security team has identified a potential risk that could impact the confidentiality and integrity of your account data.

**Vulnerability Description:**

[Brief description of the vulnerability, e.g., session hijacking, outdated app version, or API flaw].

**Required Mitigation Actions:**

- Update the [Bank Name] mobile application to version [Version Number] immediately via the official App Store or Google Play Store.
- Enable Multi-Factor Authentication (MFA) within the application settings.
- Avoid using public Wi-Fi networks when conducting financial transactions.
- Change your mobile banking PIN and password following the application update.

**Current Status:**

Our technical team is currently [deploying a patch / monitoring systems / investigating the scope]. No unauthorized access to your specific account has been detected at this time; however, these steps are necessary to ensure continued protection.

If you notice any suspicious activity or require technical assistance, please contact our Information Security Support Desk at [Phone Number] or [Email Address].

Sincerely,

[Name]

[Title]

[Bank Name] Information Security Department