

To: [Recipient Name/Legal Department/Product Team]

From: [Your Name/Security Compliance Office]

Date: [Insert Date]

Subject: ADVISORY: Potential Open Source Software (OSS) Contamination in [Product Name]

Dear [Name],

This letter serves as a formal advisory regarding the identification of open source software (OSS) components within the [Product Name] codebase that may conflict with our intellectual property standards or licensing obligations.

1. Identification of Issue

During a recent [Software Composition Analysis (SCA) / Code Audit], the following components were identified as potentially "contaminating" the proprietary supply chain:

- **Component Name:** [e.g., Library-X]
- **Version:** [e.g., v2.4.1]
- **License Type:** [e.g., GPL v3.0, AGPL]
- **Location/Path:** [Insert Directory Path]

2. Nature of Risk

The identified components carry licenses categorized as [Copyleft / Restricted / Non-Compliant]. Use of this code in its current form may require the disclosure of our proprietary source code or create legal liabilities regarding distribution rights.

3. Required Remediation Actions

The [Product/Development] team is requested to perform one of the following actions by [Deadline Date]:

- **Replacement:** Substitute the component with a commercially friendly licensed alternative (e.g., MIT, Apache 2.0).
- **Isolation:** Architecturally isolate the component to prevent derivative work implications.
- **Removal:** Completely remove the code and re-implement the functionality using internal resources.

4. Verification

Upon completion of the remediation, please provide a clean scan report or a technical summary of the changes to the Compliance Office for final validation.

Failure to address this advisory may delay the release of [Product/Version Number] and impact our software supply chain integrity.

Sincerely,

[Your Signature]
[Your Title]
[Company Name]