BISHOPFOX

8240 S. KYRENE ROAD
SUITE A-113
TEMPE, AZ 85284
UNITED STATES

BISHOPFOX.COM

March 30, 2021

Time to Reply Limited
34a Cote Green Lane
Marple Bridge
Stockport
SK6 5EB
England

To Whom It May Concern:

In March of 2021, the Bishop Fox assessment team conducted a limited penetration test of the Timetoreply application and its external infrastructure, a cloud security review of its AWS environment, and a review of the responses Time to Reply Limited provided for a self-assessment questionnaire. For detailed information on the products and Google APIs in scope, please see Appendix A.

This testing was designed to support Google's platform risk management function, and as such the activities should not be considered a comprehensive assessment wholly or in part.

The engagement objective was to identify representative security issues within a time-boxed assessment. The Bishop Fox assessment team combined automated network and application scanning with limited manual penetration testing to locate weaknesses. In addition, Bishop Fox reviewed the self-assessment questionnaire completed by Time to Reply. For more information on Bishop Fox's testing approach, please see Appendix B.

This letter confirms that the testing of the Timetoreply application and external infrastructure has been completed. Time to Reply has been provided the detailed findings and recommendations resulting from the assessment in an assessment report. At the time of this letter, all critical- and/or high-risk findings have been remediated.

Testing for this engagement concluded on March 24, 2021. This letter is valid until March 30, 2022.

Sincerely,

Thomas Eston
Practice Director
Bishop Fox

Thomas Eston
Digitally signed by Thomas Eston
Date: 2021.03.30 16:46:59 -04'00'

APPENDIX A — TESTING SCOPE

Reviewed Products

This letter addresses the following product:

- Project Name: timetoreply com v2
  Google Project Number: 690320043607

API Scope Verification

The assessment team verified the application's use of the following restricted Google API scope:

- `https://www.googleapis.com/auth/gmail.metadata`

APPENDIX B — TESTING ACTIVITIES AND APPROACH

The security assessment included the following activities:

1. External Network Penetration Testing
   Identification of potential vulnerabilities in external, internet-facing infrastructure and systems such as the following:
   - Discovery and enumeration of live hosts, open ports, services, unpatched software, administration interfaces, authentication endpoints lacking MFA, and other external-facing assets
   - Automated vulnerability scanning combined with manual validation
   - Brute-forcing of authentication endpoints, directory listings, and other external assets
   - Analysis of potential vulnerabilities to validate and develop complex attack chaining patterns and custom exploits
   - Potential exploitation of software vulnerabilities, insecure configurations, and design flaws

2. Application Penetration Testing
   Identification of potential vulnerabilities in the application that access Google user data such as the following:
   - Real-world attack simulation focused on identification and exploitation
   - Discovery of attack surface, authorization bypass, and input validation issues
   - Automated vulnerability scanning combined with manual validation
   - Exploitation of software vulnerabilities, insecure configurations, design flaws, and weak authentication
   - Analysis of vulnerabilities to validate and develop complex attack chaining patterns and custom exploits
   - Verify the ability for users to delete their account with no external indication that the user or user's content is accessible.

3. Cloud Security Review
   Identification of exploits and vulnerabilities in developer infrastructure such as the following:
   - Gathering all available configuration settings and metadata as well as manual techniques to build a profile of the cloud environment
   - Analyzing collected information to identify any gaps or deviations from accepted cloud security best practices
   - Manually examining configuration settings to locate anomalies and issues such as weak IAM policies, exposed storage containers, poorly defined security groups, insecure cloud services usage, and insecure key management
   - Exploitation of vulnerabilities, insecure configurations, design flaws, and weak authentication – as needed
   - Verifying that storage of OAuth tokens is encrypted and encryption keys and secrets are stored in a hardware security module or equivalent strength key manager
   - Ensuring developer access to the deployment environment is secured with multi-factor authentication

4. Policy and Procedure Review
   Review and examination of the efficacy of information security policies and procedures such as the following:
   - Incident response plan: Establishes roles, responsibilities, and actions when an incident occurs
   - Risk management policy: Identifies, reduces, and prevents undesirable incidents or outcomes
   - Vulnerability disclosure program: Provides a means for external parties to report vulnerabilities
   - Information security policy: Ensures that all users comply with rules and guidelines related to the security of the information stored digitally at any point in the network
   - Privacy user data detection: Ensures that users can delete their accounts and related user data by demonstrating an account deletion if relevant