



TAP MOBILE SERVICES EXHIBIT

This TAP Mobile Services Exhibit is an exhibit to the General Terms and Conditions ("General Terms"). The General Terms are an integral part of this Proofpoint Nexgate Services Exhibit and are incorporated by reference.	
IN WITNESS WHEREOF, Proofpoint and Customer represent and warrant to the other that the person entering into this TAP Mobile Services Exhibit is authorized to sign this Agreement on behalf of their respective party.	
CUSTOMER:	PROOFPOINT, INC.:
Individual Signing: [print name]	Individual Signing: [print name]
Signature:	Signature:
Title:	Title:
Signing Date:	Signing Date:

1. **DEFINITIONS.** For purposes of this TAP Mobile Services Exhibit the following definitions shall apply. Capitalized terms used in this TAP Mobile Services Exhibit without separate definition shall have the meaning specified in the General Terms.

1.1 **"Apps"** means mobile device applications that Customer submits to Proofpoint for analysis under the applicable TAP Mobile Service.

1.2 **"Customer Data"** means the data uploaded by Customer to Proofpoint via the applicable TAP Mobile Service and stored on Proofpoint's servers and the rules and policies set by Customer in its use of the TAP Mobile Service.

1.3 **"Customer Equipment"** means Customer's computer hardware, software and network infrastructure used to access the TAP Mobile Service.

1.4 **"Devices"** means Customer's and its Affiliates' mobile devices that are managed by the applicable TAP Mobile Service.

1.5 **"TAP Mobile Service(s)"** means the applicable TAP mobile service(s) set forth in TAP Mobile Services Description attached hereto as Attachment A.

1.6 **"Users"** means Customer's and its Affiliates' employees, agents, contractors, consultants or other individuals who are authorized by Customer to use the TAP Mobile Services.

2. **TERMS OF TAP MOBILE SERVICE.** Proofpoint shall make the TAP Mobile Service available to Customer and its Affiliates in accordance with the General Terms, Order Form, this TAP Mobile Services Exhibit and the TAP Mobile Services Description. For the purposes of this TAP Mobile Services Exhibit, the definition of Mailbox in the General Terms shall not apply and any other reference to "Mailbox" in the General Terms shall be deleted and replaced with, as applicable (i) "Devices" and (ii) "Apps". Customer's right to use the TAP Mobile

Service is limited to, as applicable: (i) the maximum number of Devices specified in each Order Form and (ii) the maximum number of Apps specified in each Order Form.

3. **CUSTOMER RESPONSIBILITIES.** Customer is responsible for (i) all activities conducted under its User logins, including activities in violation of the Terms of Use ("TOU"), a copy of which is included under Attachment A; (ii) obtaining and maintaining any Customer Equipment and any ancillary services needed to connect to, access or otherwise use the TAP Mobile Service and ensuring that the Customer Equipment and any ancillary services are compatible with the TAP Mobile Service and comply with all configuration requirements set forth in the TAP Mobile Services Description; and (iii) complying with all laws, rules and regulations regarding the management and administration of its mobile devices and its mobile device management system, including but not limited to, obtaining any required consents and/or acknowledgements from Device users in managing its corporate mobile device system. For the avoidance of doubt, as between the parties, Customer shall be solely responsible for any damage or loss to a third party resulting from the rules and policies set by Customer.

4. **THIRD PARTY SERVICES.** The TAP Mobile Service may allow Customer to interface with a variety of third party software or services obtained separately by Customer (e.g., mobile device management solutions). No endorsement of any such service should be inferred as a result of any integration with the TAP Mobile Service and Proofpoint is not responsible for the data, operation or functionality of such third party services. Customer shall be responsible for complying with the terms and policies it has agreed to with any such third party service including, without limitation, any payment obligations

related thereto. Proofpoint cannot guarantee that such third party services will continue to interoperate with the TAP Mobile Service.

5. WARRANTIES. Proofpoint warrants that the TAP Mobile Service will substantially conform in all material respects in accordance with the TAP Mobile Services Description. Customer will provide prompt written notice of any non-conformity. Proofpoint may modify the TAP Mobile Services Description in its sole discretion, provided the functionality of the TAP Mobile Service will not be materially decreased during the Term. As Customer's sole and exclusive remedy and Proofpoint's entire liability for any breach of the foregoing warranty, Proofpoint will (i) use reasonable efforts to fix, provide a work around, or otherwise repair or replace the TAP Mobile Service or, if Proofpoint is unable to do so, (ii) terminate this TAP Mobile Services Exhibit and return the Subscription Fees paid to Proofpoint or Reseller for such allegedly defective TAP Mobile Service for the period commencing from Customer's notice of nonconformity through the remainder of the Initial Term or Extension Term, as applicable.

6. TERMINATION. Upon the effective date of termination of this TAP Mobile Services Exhibit or the Agreement, Customer's license to use the TAP Mobile Service will cease.

ATTACHMENT A

TAP MOBILE SERVICES DESCRIPTION

Overview

TAP Mobile Services is a hosted application that provides enterprises with protection and visibility against malicious and privacy-leaking .ipa (iOS) and .apk (Android) applications.

TAP Mobile Defense Service

TAP Mobile Defense Service integrates with a customer's MDM ("Mobile Device Management") solution to enable the customer to determine if mobile devices (BYOD "Bring Your Own Device" or COPE "Corporate-Owned, Personally-Enabled") connecting to the corporate network contain mobile applications that pose a security threat to the enterprise. Risky behavior may include: reading contact database, browser history, SMS logs, device information, and transmitting that information to malicious URL's or IP addresses. In order for TAP Mobile Defense Service to function properly, a customer must have a Proofpoint-supported MDM solution currently deployed.

TAP Mobile Defense Service offers an administrative console for a dashboard view of mobile applications and related risks. Customers can use the administrative console to set thresholds for risky mobile application behavior and to restrict specific mobile application behavior. Customers can designate specific mobile applications to be white listed or black listed, and can quarantine devices by requesting that access to enterprise services be restricted by the MDM service until the specific risky mobile applications are removed.

TAP Mobile Defense Service includes an optional mobile client application that works with customer's MDM or Enterprise Mobility Management platforms to inform customer's employees in a corporate BYOD environment about potential risks associated with the mobile applications on their devices.

TAP Marketplace Monitoring Service

TAP Marketplace Monitoring Service allows customers to submit mobile applications to Proofpoint for analysis for risky behavior. Proofpoint generates a mobile application risk report based on its analysis which Customer can review before any mobile application is pushed to employees or made available to consumers via private or public mobile application stores. The TAP Marketplace Monitoring Service works independently of the TAP Mobile Defense Service and currently supports .apk (Android) and .ipa (iOS) mobile applications. TAP Marketplace Monitoring Service does not require MDM integration.

TAP Mobile Services Terms of Use

1. Neither Customer nor any of its Device users shall attempt to gain unauthorized access to, disrupt the integrity or performance of, decompile, disassemble, reverse engineer or otherwise attempt to derive source code from the TAP Mobile Services.
2. Customer acknowledges that the TAP Mobile Services may access and store the email address, network identifier and mobile phone number associated with a Device. Customer therefore agrees to only use the TAP Mobile Services to process personal data in compliance with all applicable data privacy regulation (e.g., with consent or in pursuit of legitimate interests).
3. The TAP Mobile Services may, according to Customer's rules and policies, be used to instruct Customer's MDM to quarantine a user's Device or deny a user's Device access to the enterprise services.