**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Zero Technologies, Inc. | ) | **ITC-214-20170524-00102** |
| Application for Global And Limited Global | ) | |
| Resale Authority Pursuant to Section 214 | ) | |
| of the Communications Act of 1934, | ) | |
| as amended | ) | |

**PETITION TO ADOPT CONDITIONS TO AUTHORIZATIONS AND LICENSES**

The U.S. Department of Justice ("USDOJ"), to include its components, the National Security Division ("NSD") and the Federal Bureau of Investigation ("FBI"), submits this Petition to Adopt Conditions to Authorizations and Licenses ("Petition"), pursuant to Section 1.41 of the Federal Communications Commission ("Commission") rules.[1] Through this Petition, the USDOJ advises the Commission that it has no objection to the Commission approving the authority sought in the above-referenced proceeding, provided that the Commission conditions its approval on the assurance of Zero Technologies, Inc. ("Zero") to abide by the commitments and undertakings set forth in the June 27, 2018 Letter of Agreement ("LOA"), a copy of which is attached hereto.

The Commission has long recognized that law enforcement, national security, and public safety concerns are part of its public interest analysis, and has accorded deference to the views of other U.S. government agencies with expertise in those areas. *See In the Matter of Comsat Corporation d/b/a Comsat Mobile Communications, etc.*, 16 FCC Rcd 21,661, 21707 ¶ 94 (2001).

[1] 47 C.F.R. § 1.41.

After discussions with representatives of Zero in connection with the above-referenced proceeding, the USDOJ, NSD and FBI have concluded that the additional commitments set forth in the LOA will help ensure that the FBI, which has the responsibility of enforcing the law, protecting the national security, and preserving public safety, can proceed appropriately to satisfy those responsibilities. Accordingly, the USDOJ advises the Commission that it has no objection to the Commission granting the application in the above-referenced proceeding, provided that the Commission conditions its consent on compliance with the LOA.

Respectfully submitted,

SANCHITHA JAYARAM
Chief, Foreign Investment Review Staff
National Security Division
United States Department of Justice

BERMEL R. PAZ
National Security Division
United States Department of Justice
3 Constitution Square
175 N St NE, Suite 12-1805
Washington, D.C. 20002

June 28, 2018

Date 27 Jun 18

Assistant Attorney General for National Security
United States Department of Justice
National Security Division
950 Pennsylvania Avenue NW,
Washington, DC 20530

Subject: FCC # ITC-214-20170524-00102
Application by Zero Technologies, Inc. for authority to provide resale service between the United States and permissible international points.

Dear Sir/Madam:

This Letter of Agreement ("LOA" or "Agreement") outlines the commitments being made by Zero Technologies, Inc. ("Zero") to the U.S. Department of Justice ("USDOJ") in order to address national security, law enforcement, and public safety concerns raised with regard to Zero's application to the Federal Communications Commission ("FCC" or "Commission") for authority to provide resale service between the United States and permissible international points pursuant to Section 214 of the Communications Act of 1934, as amended.

Zero adopts as true and correct all statements Zero or its representatives have made to USDOJ or other Team Telecom member agencies and the FCC in the course of the review of the above-referenced application, and it hereby adopts those statements as the basis for this LOA.

1. For purposes of this LOA, the following definitions apply:

a. "Zero" means Zero Technologies, Inc. or its successors-in-interest.

b. "Access" or "Accessible" means the ability to physically or logically undertake any of the following actions: (a) to read, copy, divert, or otherwise obtain non-public information or technology from or about software, hardware, a database or other system, or a network; (b) to add, edit, delete, reconfigure, provision, or alter information or technology stored on or by software, hardware, a system or network; and (c) to alter the physical or logical state of software, hardware, a system or network.

c. "Classified Information" shall have the meaning indicated by Executive Order 13526 and the Atomic Energy Act of 1954, or any subsequent Executive Order or statute regarding the same.

d. "Customer Proprietary Network Information" (CPNI) shall mean as defined in 47 U.S.C. § 222(h)(1).

e. "Date of this LOA" shall mean the date on which the Letter of Agreement is executed by Zero.

f. "Domestic Communications," as used herein, means: (1) Wire Communications or Electronic Communications (whether stored or not) from one U.S. location to another U.S. location; and (b) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States.

g. "Domestic Communications Infrastructure" (DCI) means any systems, equipment, hardware, software or applications that capture or control, or transmit the flow of Domestic Communications on behalf of Zero, including information technology supporting such networks.

h. "Electronic Communication" has the meaning provided in 18 U.S.C. § 2510(12).

i. "Electronic Surveillance" means: (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. § 2510(1), (2), (4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (b) Access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 et seq.; (c) acquisition of dialing, routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 et seq. and 50 U.S.C. § 1841 et seq.; (d) acquisition of location-related information concerning a subscriber or facility; (e) preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and (f) access to or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (a) through (e) above and comparable state laws.

j. "Foreign" means non-United States.

k. "Geolocation Data" means any information collected by Zero from its customers regarding a customer or the customer's device location.

l. "Government" means any government, or governmental, administrative, or regulatory entity, authority, commission, board, agency, instrumentality, bureau or political subdivision, and any court, tribunal, judicial or arbitral body.

m. "Internet Search Information" includes any data collected by Zero about its customer's internet browsing or online purchasing activities through any mechanism permitted by the services offered by Zero.

n. "Lawful U.S. Process" means U.S. federal, state, or local court orders, subpoenas, warrants, processes, directives, certificates or authorizations, and other orders, legal process, statutory authorizations and certifications for electronic surveillance, physical search and seizure, production of tangible things or access to or disclosure of Domestic Communications, call-associated data, transactional data, subscriber information, or associated records.

o. "Managed Network Service Provider" means any third party using an end-to-end or managed services platform that has the ability to access or control Domestic Communications to or from Zero's customers or users.

p. "Network Elements" means a facility, equipment, software, hardware or applications used in the provision of telecommunications services, including features, functions and capabilities that are provided by means of such facility or equipment, including subscriber numbers, databases, signaling systems, and information sufficient for billing, receiving and/or aggregating customer data, and collection or used in the transmission, routing, or other provision of telecommunications services.

q. "Network Management Capabilities" means software or applications used to manage or monitor network operations.

r. "Network Operations Center" means any locations and facilities performing network management, monitoring, accumulation of accounting and usage data, maintenance, user support, or other operational functions for Domestic Communications.

s. "Non-US Government" means any government, including an identified representative, agent, component or subdivision thereof, that is not a local, state, or federal government in the United States.

t. "Offshoring" means performing obligations of this Agreement through the use of entities and personnel outside of the territorial limits of the United States, whether those entities or personnel are employees of Zero or its subsidiaries, or third parties.

u. "Outsource" or "Outsourcing" means, with respect to Domestic Communications, supporting the services and operational needs of Zero at issue in this LOA through the use of contractors or third parties.

v. "Principal Equipment" means any equipment, hardware, software, or applications capable of controlling Domestic Communications, as well as device controllers, signal routing and transfer routers, devices that perform network or element management, fiber optic line termination and multiplexing, core and edge routing, network protection, radio network control, mobility management, or lawful intercept functions, and non-embedded software necessary for the proper monitoring, administration and provisioning of any such equipment. This definition may be modified from time to time by USDOJ as may be necessary due to changes in technology, business model, management, structure of services offered, or governance of the Domestic Communications.

w. "Security Incident" means (a) any known breach or suspected breach of the Agreement, including a violation of any Network and Systems Security Plan or use of Outsourced or Offshore service providers or Network equipment (b) any known exploitation or suspected exploitation of a security vulnerability.

x. "U.S. Records" means Zero's customer billing records, subscriber information, text, Internet Search Information online purchasing information, or Geolocation Information, CPNI, and any other related information used, processed, or maintained in the ordinary course of business relating to the services offered by Zero in the United States, including information subject to disclosure to a U.S. federal or state governmental entity under the procedures specified in 18 U.S.C. § 2703(c) and (d) and 18 U.S.C. § 2709.

y. "Wire Communication" has the meaning provided in 18 U.S.C. § 2510(1).

2. Zero confirms that it will comply with all applicable lawful interception statutes, regulations, and requirements, including the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. 1001 *et seq.*, and its implementing regulations, as well as comply with all court orders and other Lawful U.S. Process for lawfully authorized Electronic Surveillance.

3. Upon receipt of any Lawful U.S. Process, Zero shall place within the territorial boundaries of the United States any and all information requested by the Lawful U.S. Process within the period of time for response specified in the Lawful U.S. Process, or as required by law, and shall thereafter comply with the Lawful U.S. Process.

4. Zero agrees to notify USDOJ, at least 30 days in advance, on any change to its current services portfolio or any peering relationships or joint ventures with foreign companies providing data aggregation or reselling services.

5. Zero agrees that it will not, directly or indirectly, disclose or permit disclosure of or Access to U.S. records or domestic communications or any information (including call content and call data) pertaining to a wiretap order, pen/trap and trace order, subpoena, or any other Lawful U.S. Process demand if the purpose of such disclosure or access is to respond to the legal process or request on behalf of a non-U.S. Government entity without first satisfying all pertinent requirements of U.S. law and obtaining the express written consent of USDOJ, or the authorization of a court of competent jurisdiction in the United States. Any such requests for legal process submitted by a non-U.S. Government entity to Zero shall be referred to USDOJ as soon as possible, but in no event later than five (5) business days after such request or legal process is received by or made known to Zero, unless disclosure of the request or legal process would be in violation of U.S. law or an order of a court of competent jurisdiction in the United States.

6. Zero agrees to draft: (1) a NIST-Compliant Cyber Security Plan; and (2) Network Systems Security Plan ("NSSP"), which will be forwarded to USDOJ within 60 days of the Date of this LOA for objection or non-objection. The NSSP shall address, but not be limited to, information security, remote access, physical security, cyber-security, third-party contractors,

Outsourcing and Offshoring, maintenance and retention of system logs, protection of Lawful U.S. Process, protection of U.S. Records obtained by Zero from their customers or through the provision of services, and Zero's specific plan regarding new contracts or any amendments any existing contracts with third-party providers of services to require those third parties to notify Zero in the event of a breach or loss of U.S. Records within a specified time period after discovery, not to exceed five (5) business days from the date of discovery.

7. Zero agrees to require any third-party provider of services to disclose any data breach of any U.S. Records, or any loss of U.S. Records, whether from a data breach or other cause, within 48 hours of the third party discovering the breach or loss. To the extent that Zero has current agreements with any third-party providers of services with access to U.S. Records, Zero agrees to amend those agreements to require those third parties to make disclosure of breaches or loss of U.S. Records consistent with this paragraph, and shall forward copies of those amended agreements to USDOJ points of contacts listed in paragraph 15 within five (5) business days of executing those amendments.

8. Zero agrees to notify the Federal Bureau of Investigation ("FBI") and the U.S. Secret Service within seven (7) days upon learning that a person or entity without authorization, or in exceeding their or its authorization, has intentionally gained access to, used, or disclosed any of its customer's CPNI or that of a third party used by Zero, and shall report the matter to the central reporting facility through the following portal:

https://www.cpnireporting.gov/cpni/content/disclaimer.seam

9. Zero agrees to designate and maintain a U.S. law enforcement point of contact ("LEPOC") in the United States who will be subject to prior approval by the USDOJ, including the FBI. The LEPOC shall be a U.S. citizen residing in the United States unless USDOJ agrees in writing otherwise, and the LEPOC must be approved by the FBI to receive service Lawful U.S. Process for U.S. Records and, where possible, to assist and support lawful requests for surveillance or production of U.S. Records by U.S. federal, state, and local law enforcement agencies. This LEPOC and his/her contact information will be provided to USDOJ within 15 days from the date Zero receives the FCC's approval of the transfer. Zero also agrees to provide USDOJ at least 30 days prior written notice of any change in its LEPOC, with all such changes subject to the approval of USDOJ, including the FBI. In addition, Zero will give USDOJ, including the FBI, at least 30 days prior written notice of any change to its LEPOC, and Zero's nominated replacement shall be subject to USDOJ, including the FBI, review and approval. Zero also agrees that the designated LEPOC will have access to all U.S. Records, and, in response to Lawful U.S. Process, will make such records available promptly and, in any event, no later than five (5) business days after receiving such Lawful U.S. Process unless granted an extension by NSD.

10. Zero agrees to notify USDOJ, including the FBI, at least 30 days in advance, of any introduction of new Principal Equipment or changes/modification to any of its Principal Equipment, including the names of providers, suppliers, and entities that will perform any maintenance, repair, or replacement that may result in any material modification to its Principal Equipment or systems or software used with or supporting the Principal Equipment. USDOJ shall object or non-object to such new Principal Equipment or change/modification to the Principal Equipment within 30 days of receipt of notice.

11. Zero agrees to notify the USDOJ, including the points of contact (POC) listed in paragraph 16, of any breaches of this agreement, as well as any other Security Incidents such as, but not limited to cyber-security incidents, intrusions or breaches of Network Elements. The notification shall take place no later than 15 days after Zero or any third party providing Outsource or Offshore services to Zero discovers the incident, intrusion or breach takes place, or sooner when required by statute or regulations.

12. Zero agrees to permit USDOJ requests for site visits and approve all requests to conduct on-site interviews of Zero employees.

13. Zero further agrees that it will provide USDOJ notice at least 30 days in advance of all Outsourced or Offshore service providers, including but not limited to services provided in relation to:

- Network operation center(s) ("NOC");
- Network maintenance services;
- Customer support services;
- Any operation/service that could potentially expose U.S. domestic telecommunications infrastructure, U.S. customer data and records, call detail records ("CDRs"), or CPNI; and
- Deployment of any network elements, hardware, software, core network equipment, and network management capabilities that are owned, managed, manufactured or controlled by a foreign government or non-public entities.

USDOJ shall object or non-object to Outsourced or Offshore service providers, within 30 days of receipt of notice.

14. Zero agrees to provide USDOJ with notice of any changes to its business, including but not limited to corporate structure changes , ownership changes, corporate name changes, business model changes, corporate headquarter location changes, or business operation location changes within 30 days in advance of such change.

15. Zero agrees to designate one individual as "Compliance Officer" to oversee compliance with the terms of this LOA, who shall be a person at the executive-level of the company with sufficient experience, and Zero shall notify USDOJ of the identity of this individual no later than 15 days after the Date of this LOA.

16. Zero agrees to provide an annual report to USDOJ regarding the company's compliance with this Agreement, to include:

- Certifications that there were no changes (where no changes were reported to USDOJ, including the FBI, during the preceding year);
- Certification that Zero has been in CALEA compliance;
- Notice(s) regarding the company's handling of U.S. Records, Domestic Communications, and Lawful U.S. Process (i.e., whether handled properly and in

accordance with the assurances contained herein) including list of individuals with access to U.S. CDRs;

- Recertification on any changes in the services that Zero provides or confirmation that no additional services are being offered;
- Notification(s) of any relationships with foreign-owned telecommunications partners, including any peer relationships;
- Updated list of Zero's Principal Equipment, vendors and suppliers;
- Updated Network and Systems Security Plans and Procedures;
- Updated NIST-Compliant Cyber Security Plan;
- Notification(s) of the installation and/or purchase or lease of any foreign-manufactured telecommunication equipment (including, but not limited to, switches, routers, software, hardware);
- Report(s) of any occurrences of cyber-security incidences, network and enterprise breaches, and unauthorized access to customer data and information;
- A re-identification of the name of and contact information of the LEPOC; and
- Notifications regarding any other matter of interest to this LOA.

The annual report will be due every 31st day of January of each calendar year, beginning on January 31, 2019, and will be addressed to:

Assistant Attorney General for National Security
U.S. Department of Justice
National Security Division
Three Constitution Square, 175 N Street NE,
Washington, DC 20002

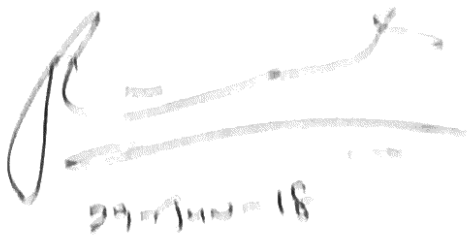
Attention: FIRS/Team Telecom Staff

Courtesy electronic copies of all notices and communications will also be sent to the following or individuals identified in the future to Zero by USDOJ: Bermel Paz, USDOJ (at Bermel.Paz@usdoj.gov); Joanne Ongman, USDOJ (at joanne.ongman@usdoj.gov), Loyaan Egal, USDOJ (at Loyaan.Egal@usdoj.gov) and FIRS Team (at FIRS-TT@usdoj.gov).

17. Zero agrees that in the event that the commitments set forth in this letter are breached, USDOJ may request the FCC to modify, condition, revoke, cancel, or render null and void any relevant license, permit, or other authorization granted by the FCC to Zero or its successors-in-interest, in addition to any other remedy available at law or equity.

18. Zero understands that, upon execution of this LOA by an authorized representative or attorney, or shortly thereafter, USDOI shall notify the FCC that it has no objection to the FCC's consent to Zero's application.

Sincerely,



Name/Title/Date
**Zero Technologies, Inc.**