Anti-Money Laundering Policy
Radius Global Infrastructure, Inc. and its Subsidiaries

Last updated: October 2, 2020

Purpose, scope and responsibility

Radius Global Infrastructure, Inc. ("Radius") and its subsidiaries (collectively, the "Company") are subject to various anti-money laundering (AML) laws, regulations, requests and requirements relevant to the specific business and jurisdiction where the business operates. This policy recognizes the need for awareness by the Company to comply with such laws and regulations and to fulfill such requirements and requests, as applicable, including risk-based Know Your Customer (KYC) policies and procedures and requests from lenders and other banking and financial institutions with whom the Company may transact or be engaged with for business.

This policy applies to all employees of the Company, and business units or individual subsidiaries may adopt AML policies specifying additional AML compliance requirements and procedures in accordance with applicable laws of the locations where each does business or is located.

The General Counsel of the Company is the final authority for this policy.

Policy Statement

Radius established this AML policy in conjunction with its other corporate policies to help detect transactions that may involve money laundering, terrorist financing, or other illicit activity, and to provide resources for reporting applicable situations as required by applicable law or as required by third parties for business engagement. This policy also helps ensure the Company satisfy all legal and regulatory requirements and maintain ethical business practices.

Each of Radius and its subsidiaries is subject to various AML laws and regulations depending on the nature of the business and the country in which such entity is domiciled or conducting business.

Each of the Radius subsidiaries outside the U.S. must comply with all requirements of the laws and regulations of relevant jurisdictions applicable to their business, including applicable U.S. laws. This policy focuses on summarizing AML requirements under U.S. law.

The Company's General Counsel shall monitor and support compliance with this policy and regularly report to senior management, including the Audit Committee of the Board of Directors.

U.S. Anti-Money Laundering Program Requirements

The Bank Secrecy Act, as modified by the USA PATRIOT Act (Act) on Oct. 26, 2001 (collectively the "BSA"), sets forth the requirements imposed on financial institutions to facilitate the prevention, detection, and prosecution of international money laundering and the financing of terrorism. The BSA requires U.S. financial institutions such as banks, securities broker-dealers, mutual funds, insurance companies, and other financial services businesses to establish formal AML programs. Although the Company is not deemed a financial services businesses governed by the BSA, the Company frequently engages with lenders, banks, and other third parties throughout the countries in which it operates who, as a result of their own AML policies and legal requirements, require that the Company respond to specific requirements and requests,

including certification of its own AML and KYC policies and processes.

Subject to conforming to industry specific regulations, these AML policies are generally required to address the following:

- Collecting and verifying appropriate identifying information about customers, beneficial owners, and control persons and maintaining records of such information (a "control person" is someone who has a level of control over, or entitlement to, the funds or assets that, as a practical matter, enable the person, directly or indirectly, to control, manage, or direct the account/or on whose behalf a transaction/activity is being conducted);
- Comparing the names of customers, beneficial owners, business associates, and payees with the lists maintained by the Financial Crimes Enforcement Network (FinCEN), a division of the U.S. Treasury Department and the Office of Foreign Assets Control (OFAC) (and any other similarly mandated lists) and reporting any matches or otherwise complying with legal requirements;
- Refusing to accept funds from, or to do business with, shell banks or customers whose funds the company should reasonably believe are derived from criminal activity or from a sanctioned source;
- Training employees, agents, and brokers to identify red flag activities and report them to their manager or as directed in their AML procedures;
- Designating an AML Compliance Officer who, in conjunction with applicable compliance personnel, will review red flag activities and determine appropriate measures to take, consistent with applicable law. Examples of measures include refusing to open an account, severing relations with the customer or vendor, closing or freezing accounts, and, when appropriate, filing a suspicious activity report (SAR) with FinCEN;
- Understanding the nature and purpose of the customer relationships and implementing appropriate risk-based procedures for conducting ongoing due diligence; and
- Conducting annual independent audits to evaluate the effectiveness of the Company's AML policies and procedures.

The Company's General Counsel, along with the legal and finance departments, have developed and implemented AML programs tailored to address the risks specific to the Company's business.

Suspicious Activity Reporting/CompanyContacts

All Company employees and representatives must report all suspicious transactions in writing to the Company's General Counsel, either directly or through their supervisor or other member of the legal department. Supervisors will coordinate suspicious transaction information with the Company's General Counsel.

Accountabilities

All Company employees and representatives are responsible for knowing and following all applicable AML, OFAC, and similar jurisdiction-specific policies and procedures. They should:

- Be familiar with the AML, OFAC, and other policies in the jurisdictions in which they operate;
- Be familiar with any specific AML or other policies required by law in the jurisdictions in which they operate, including
    - All verification (KYC) procedures for opening new bank accounts and servicing existing bank accounts.
    - How to flag activities that may require special attention, trigger reporting requirements,

and/or need special approval.

- Report red flag activities or suspicious transactions as directed.