PlanetShop, Inc.

ANTI-MONEY LAUNDERING COMPLIANCE MANUAL

Last Updated: April 13, 2022

Chief Compliance Officer Keren Tamara Gordon
Phone Number:+1 (818) 317 - 5888 Email: alexx6686@gmail.com

Table of Contents

Chapter 1: Adoption of Compliance Program

A. Purpose of Compliance Program

It is the policy of PlanetShop, Inc. (the "PlanetShop", "Company," "our," "us," or "we") to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act ("BSA") and its implementing regulations. This Anti-Money Laundering Compliance Program Manual ("Manual") is designed to provide guidelines to Company employees on the purpose of our anti-money laundering compliance program and their obligations thereunder.

Our anti-money laundering ("AML") policies, procedures, and internal controls are designed to ensure compliance with all applicable BSA rules and regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

This Policy was approved and implemented as of February 15, 2017 and shall be updated periodically, with all changes recorded in the Change Log in Section B. The Company is required to register as a Money Service Business ("MSB") with the Financial Crimes Enforcement Network ("FinCEN") as an exchanger and money transmitter. *See Rules:* 31 U.S.C. § 5318; 31 C.F.R. § 1022.

B. Change Log

The change control log tracks the progress of each change to the PlanetShop's Compliance Policy.

Version	Change Date	Author	Summary of Changes
1.1	February 15, 2017	Rafael Yakobi	Created New Policy
1.2	June 24, 2020	Sasha Hodder	Added to the KYC/CDD/Record Retention Sections
1.3	July 16, 2020	Sasha Hodder	Removed a Typo, Edited Surveillance Monitoring Policy to be more accurate with current practices of the Company.
1.4	March 23, 2022	Sasha Hodder	Changed the following: (1) Added criteria to the EDD Policy, (2) Added additional information on the OFAC Obligations and (3) Update of MSB Registration Details

C. Designation of Compliance Officer

The Company has formally designated a Chief Compliance Officer ("CCO"). The designated employee will be in a position of responsibility that allows them to implement an effective Anti-Money Laundering Compliance Program (the "Program"). The CCO is responsible for ensuring the on-going compliance of this money services business ("MSB") with all federal and state anti-money laundering laws and regulations. The Company designates Keren Tamara Gordon as its Chief Compliance Officer. Keren Tamara Gordon has a working knowledge of the BSA and is qualified to oversee the AML Program.

The CCO's duties include:

(1) Ensuring the day-to-day compliance with the Program and with BSA rules and regulations as well as any applicable state rules and regulations;
(2) Monitoring PlanetShop's transactions;
(3) Responding to law enforcement requests;
(4) Ensuring that the Company properly files reports and creates and retains records in accordance with BSA regulations;
(5) Updating the Program as necessary to reflect any changes in laws, regulations, or related guidance from the Department of the Treasury;
(6) Ensuring that the Company provides appropriate employee training and education; and
(7) Maintaining compliance with licensing laws and OFAC requirements.

The Compliance Officer is also responsible for ensuring that a periodic review is conducted on the quality of the Compliance Program. This review may not be conducted by the Compliance Officer or a qualified delegate. The review should be done by a senior level employee or qualified professional who understands the requirements of an effective compliance plan. *See Rule:* 31 C.F.R. § 1022.210(d).

D. Senior Management

PlanetShop's Senior Management, Alexander Spayev is responsible for approving the Policy and associated initiatives. Senior Management are responsible for the overall performance of the initiatives associated with the Policy, including day-to-day operations, training, transaction monitoring, ensuring the independent audit takes place annually, and implementing any updates.

E. Independent Review

Every Money Service Business (MSB) must conduct an independent review of its AML compliance program to ensure the company has established adequate compliance policies, procedures, and internal controls. The CCO is responsible for ensuring that an independent review is conducted at least once every twelve (12) months. The CCO must NOT conduct the review. Upon completion of the independent review, the person conducting the review will report its findings to the Company's senior management who will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

The independent review will include:

- Evaluation of the overall integrity and effectiveness of the compliance program;
- Evaluating the various written policies in the program;
- Review the transaction monitoring, KYC/CDD, SAR and CTR Policies and their application;
- Evaluating whether any law enforcement requests have been responded to properly;
- Evaluating the adequacy of the staff training program;

The Independent Review will include recommendations for improvements that the Company is expected to evaluate and implement within in a reasonable time. *See Rule: 31 C.F.R. § 1022.201(d)(4).*

F. Employee Training

The Company will provide ongoing AML employee training under the leadership of the CCO and senior management. The training will occur at least annually, and training materials will be updated to reflect any new developments in the law. At a minimum, the training will include:

(1) How to identify red flags and signs of money laundering that arise during the course of the employees' duties;
(2) What to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SARs);
(3) What employees' roles are in the firm's compliance efforts and how to perform them;
(4) The firm's record retention policy; and
(5) The disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

The Company will maintain records to show the persons trained, the dates of training, and the source utilized (in person, online, quiz score, pamphlets, etc. (if applicable).

All new employees will be required to read this manual and sign a copy of the Acknowledgement by Employee that will be retained in their personnel file and Anti-Money laundering files. *See Rule: 31 C.F.R. § 1022.210(d)(3).*

G. Written Know Your Customer (KYC)/Customer Due Diligence (CDD) Policy

This KYC/CDD Policy is designed to mitigate the risk of PlanetShop being used by criminals for money laundering activities. The KYC/CDD Policy enables PlanetShop to know and understand its customer by collecting and recording certain information from each customer who performs a transaction.

The Company uses a tiered system for identity verification, so the information collected from each customer corresponds to the size (or risk) of the transaction. If the customer chooses not to fulfill the identity verification requirements, the transaction will not be completed. The same identity verification information collected will also be used to perform OFAC and sanction list screening and to perform SARs and CTRs as necessary. This implementation allows the company to fulfill transactions with trusted users and record accurate transaction information for record-

keeping purposes. If a customer performs multiple transactions in a single business day, those transactions are aggregated. *See Chapter 3, Section A* for the transaction limits.

H. Written Enhanced Due Diligence (EDD) Policy

PlanetShop performs Enhanced Due Diligence (EDD) to combat the increased exposure to money laundering and/or terrorist financing posed by higher-risk customers.

Higher risk customers are identified based on their transaction activity. A customer becomes "high risk" if they:

- Have ever performed a transaction deemed worthy of a SAR filing;
- Use a cryptocurrency wallet flagged for being associated with illegal activity;
- Customers who have used a cryptocurrency wallet that has been flagged by law enforcement as being associated with illegal activity;
- Customers who have been the subject of a law enforcement inquiry;
- Customers who provide identification information that does match the information provided in previous transactions; and
- Any other reason based on the Compliance Officer's discretion

If a customer is deemed higher risk, their transactions will be reviewed more closely throughout their relationship with PlanetShop. If the customer refuses to provide certain requested information, PlanetShop will stop servicing that client. Once on the EDD list, the Compliance Officer will perform an EDD Assessment of the customer's transaction history every six months. The Assessments will be stored in a separate folder and retained for five years.

During an EDD Assessment, the Compliance Officer will review and create a report of the following:

1. How many transactions did the customer perform in the past six months?
2. What was the total volume of the transactions?
3. Does customer's KYC/CDD information match what has been provided in previous transactions? (If no, does the change look suspicious? Possibly call the client to inquire & make note of conversation.)
4. Recommendations for additional controls, such as lowering the transaction limit for this customer;
5. A decision whether or not to file a SAR.

See Chapter 3, Section A for the transaction limits.

I. Written Surveillance & Monitoring Policy

PlanetShop has established this Surveillance & Monitoring Policy to identify potential suspicious or unusual activity and determine if a SAR filing is needed.

The Compliance Officer uses her own internal reports and manual screening. The Compliance Officer will review the transaction and if there is any risk factors, she will make a decision of whether or not to file a SAR. If a SAR is deemed necessary, she will document the abnormal circumstances and follow the Company's SAR Policy.

Criteria. The following criteria are used to create an internal flag as potentially suspicious activity:

1. Has the customer performed more than two transactions in a 24-hour period for an aggregate amount greater than $1,000?
2. Has the customer performed more than two transactions in a 24-hour period for an aggregate amount greater than $10,000?
3. Has the customer performed more than five transactions in a 30-day period, for an aggregate amount greater than $10,000?
4. Has the customer performed two or more transactions in a 30-day period using different identification verification information?
5. Have two or more customers performed transactions in a 30-day period using the same phone number?
6. Has the customer refused to provide verification information when prompted?
7. Has the customer "structured" their transactions to avoid providing verification information?
8. Does the transaction activity make business sense?
9. Does the customer appear to be acting on behalf of a third party?

J. Written Identification Requirements

Before the Company completes the transaction, the Company and each director, officer, employee, or agent that engages with a potential customer **must verify and record the name and address** of the individual or business presenting the transaction before providing the individual or business with any services.

PlanetShop will obtain the following information from the customer in connection with the reportable transaction.

a. Customer's Name, Address, Date of Birth, and SSN;
b. A copy of a valid photo-bearing government identification ("ID")

If the individual is an alien or is not a resident of the United States, the Company MUST examine and record the individual's passport, alien identification card, or other official document evidencing nationality or residence. The same identity verification information collected will also be used to perform OFAC and sanction list screening and to perform SARs and CTRs as necessary.

Chapter 2: An Overview of Money Laundering and Regulatory Agencies

A. What is Money Laundering?

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three steps: placement, layering, and integration. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at

financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

B. What is a Money Services Business?

Federal regulations define "money services business" as any one of the following persons who, whether or not on a regular basis or as an organized or licensed business, is a dealer in foreign exchange, a check casher, an issuer or seller of traveler's checks or money orders, a provider of prepaid access, a seller of prepaid access, or a money transmitter. A "money transmitter" is, in a nutshell, a person that accepts currency, funds, or other value that substitutes for currency from one person and transfers, transmits, or sends the currency, funds, or other value that substitutes for currency to another person. The Company's activities include transferring, transmitting, or otherwise sending and receiving currency, virtual or otherwise, to various other parties and cryptocurrency exchanges, and exchange it on behalf of its customers. These activities qualify the PlanetShop as a money transmitter and thus money services business under federal law. *See Rules*: 31 C.F.R. §§ 1010.100(ff), 1010.100(ff)(5); *See Guidance*: FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013).

C. MSB Registration

As a money transmitter, the Company must register as an MSB with the Financial Crimes Enforcement Network ("FinCEN") and must renew this registration every two years. FinCEN is a bureau of the U.S. Department of the Treasury that collects and analyses information about financial transactions to detect and combat money laundering and terrorist financing. The rules promulgated under the BSA mandate that MSBs register with FinCEN through the BSA E-filer system. It is the duty of the CCO to renew the Company's MSB registration through the BSA E-filer system. *See Rule*: 31 C.F.R. § 1022.380.

D. Office of Foreign Assets Control

The Office of Foreign Assets Control ("OFAC") is a bureau of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against countries, regimes, organizations, and individuals. OFAC issues the Specially Designated Nationals and Blocked Entities List ("SDN List") which includes

names of companies and individuals who are connected to sanctions targets. The Company is prohibited from dealing with SDNs wherever they are located and all SDN assets must be blocked. *See Rule*: 31 C.F.R. §§ 501.601-501.606.

E. Privacy

The Gramm-Leach-Bliley Act (the "GLBA") is also known as the Financial Modernization Act of 1999. It is a United States federal law, enforced by the Federal Trade Commission ("FTC") that requires financial institutions to explain how they share and protect their customers' private information. To be GLBA compliant, financial institutions must communicate to their customers how they share the customers' sensitive data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers' private data in accordance with a written information security plan created by the institution.

Chapter 3: Reporting and Recordkeeping

A. Information to Record.

1. OFAC Obligations.

The purpose of this Export Control and Sanctions Compliance Policy (the "OFAC & Sanctions List Screening Policy") is to facilitate compliance by with all applicable export control and trade sanctions laws, including, but not limited to, the U.S. Export Administration Regulations, U.S. sanctions regulations administered by the U.S. Department of the Treasury's Office of Foreign Assets Control, and similar applicable laws in any other jurisdictions where the Company conducts business (collectively, "Export and Sanctions Laws").

Before engaging in a transaction of any amount with a customer, the Compliance Officer will determine whether the customer's name appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by the Treasury, through the Office of Foreign Assets Control or other similar body, in consultation with the Federal functional regulations. These lists include the OFAC List and the Specially Designated National ("SDN") List. The Sanctions List is available at https://sanctionssearch.ofac.treas.gov/.

In the event a match is determined, PlanetShop will refuse any pending or future transactions, and, if required, report the transaction as needed. If an individual is in this category, PlanetShop will call the OFAC hotline number 1-800-540-6322. The Company will not transact any business with a customer or individual presenting the transaction who appears on the Sanctions List.

2. Information to Record.

Transaction Tiers	Customer Information to Record	Record Retention	Report Required?
Transaction Less Than $250 USD	▪ Name ▪ Phone number ▪ State of residence ▪ Amount of Transaction ▪ Date of Transaction	1 Year	None unless suspicious per guidance in its AML Policy,
Transaction $250 - $2,999	▪ Name ▪ Phone Number ▪ Address ▪ Amount of Transaction ▪ Date of Transaction ▪ Copy of Government Photo ID	1 Year	None unless suspicious per guidance in its AML Policy
Transaction $3,000 – $9,999	▪ Name ▪ Phone Number ▪ Address ▪ Amount of Transaction ▪ Date of Transaction ▪ Copy of Government ID ▪ Payment instructions received from the client ▪ Name of the client's financial institution ▪ If provided, any of the following items: – Bank account number associated; and – Any other specific identifier of the recipient.[4]	3 Years	None unless suspicious per guidance in its AML Policy
Transaction(s) Equal To or Greater Than $10,000.00 USD	▪ Name ▪ Phone Number ▪ Address ▪ Amount of Transaction ▪ Date of Transaction ▪ Copy of Government ID ▪ Payment instructions received from the client ▪ Name of the client's financial institution ▪ If provided, any of the following items: – Bank account number associated; and – Any other specific identifier of the recipient.[4] ▪ Social Security Number or EIN. (If no SSN or EIN (because foreign or non-citizen), then copy of foreign passport.	5 Years	Currency Transaction Report if involving cash.

B. Suspicious Activity Reporting

1. When to File SARs.

The Company must file Suspicious Activity Reports ("SARs") when a transaction:

(1) Is conducted or attempted by, at, or through the Company;
(2) Involves or aggregates funds or other assets (including virtual currencies) of at least USD $2000.00; and
(3) The Company **knows, suspects, or has reason to know or suspect** that the transaction (or pattern of transactions of which the transaction is a part):
    (a) Involves funds from illegal activity or is intended to hide or disguise funds or assets derived from illegal activity;
    (b) Is designed, whether through structuring or other means, to evade or avoid this Company's recordkeeping or reporting requirements;
    (c) Serves no business or apparent lawful purpose, and the Company knows of no reasonable explanation for the transaction after examining the available facts; or,
    (d) Uses the Company to facilitate criminal activity.

The Company must file SARs **no later than thirty (30) calendar days** after the date the Company first detected the suspicious activity. If the situation requires immediate attention (such as ongoing money laundering schemes), the Company shall immediately notify by telephone an appropriate law enforcement agency (be it local police or the FBI) in addition to filing a SAR.

If the Company suspects that the suspicious activity relates to terrorist activity, it may call FinCEN's Financial Institutions Hotline at 1-866-556-3974 in addition to timely filing a SAR.

The Company may file a SAR of any suspicious transaction the Company believes is relevant to the possible violation of any law or regulation, but whose reporting is not required as stated above.

2. Examples of Suspicious Activity.

Here are some examples of suspicious activity:

1. A customer asks an employee how to avoid reporting requirements;
2. A customer threatens or bribes an employee to avoid providing ID;
3. A customer (or group of customers working together) engages in one or more transactions that fall just below the $10,000 recordkeeping and reporting threshold with the purpose of evading the Currency Transaction Reports requirements. (This practice is called structuring (see more about this in section 5 D. below); or,
4. A customer conducts transactions that are unusually large based on their history, employment, or level of income.

3. Where to File SARs.

The Company, via the CCO, shall file SARs with FinCEN through the BSA E-filer system and conduct a review for suspicious activity every two weeks.

4. Retention of SARs Records.

The Company shall maintain a copy of any SAR filed and the original record of any supporting documentation (*e.g.*, photocopies of IDs or passports) for at least **five (5) years** from the date of filing the SAR. The Company shall make these records available to FinCEN or any Federal, State, or local law enforcement agency or any Federal or State regulatory authority that examines or requires that the Company comply with the BSA.

5. Confidentiality of SARs Reports.

A SAR and any information that would reveal the existence of a SAR are confidential. If the Company or any of its directors, officers, employees, or agents are subpoenaed or requested to disclose a SAR or any information that would reveal the existence of a SAR, the Company or any of its directors, officers, employees, or agents must decline to produce the SAR or such information, citing 31 C.F.R. § 1022.230(d)(1) and 31 U.S.C. § 5318(g)(2)(A)(i), and must notify FinCEN of any such request and its response.

However, the Company or any of its directors, officers, employees, or agents may share information in the following circumstances as long as the no person involved in any reported suspicious transaction is notified that the transaction has been reported.

(1) The Company or any of its directors, officers, employees, or agents may share a SAR, or any information that would reveal the existence of a SAR, with any Federal, State, or local law enforcement agency or any Federal or State regulatory authority that examines or requires that the Company comply with the BSA.

(2) The Company or any of its directors, officers, employees, or agents may share the underlying facts, transactions, and documents upon which a SAR is based, including but not limited to, disclosures to another financial institution, or any employee or agent of another financial institution, for the preparation of a joint SAR.

(3) The Company or any of its directors, officers, employees, or agents may share a SAR or any information that would reveal the existence of a SAR within the Company's corporate organizational structure.

For more information on completing and submitting SARs Reports, see the "FinCEN SAR XML SCHEMA USER GUIDE." The most recent version of this document is available at: https://bsaefiling.fincen.treas.gov/docs/XMLUserGuide_FinCENSAR.pdf. *See Rule:* 31 C.F.R. § 1022.320.

C. Currency Transaction Reporting

1. When to File CTRs.

The Company ***must*** file a Currency Transaction Report ("CTR") of each deposit, withdrawal, exchange of currency (including virtual currencies), or other payment or transfer, by, through, or to the Company which involves a transaction in currency of more than $10,000.00 USD ***unless*** the transaction occurs is between the Company and a commercial bank, in which case a CTR is NOT required.[5]

The Company will treat multiple currency transactions as a single transaction if the Company has knowledge that the transactions are by or on behalf of any person and result in either cash-in or cash-out totaling more than $10,000.00 USD during any one business day.

The Company must file CTRs **no later than fifteen (15) calendar days** after the day on which the transaction occurred.

2. Identification Required.

Before concluding a transaction with respect to which the Company must file a CTR, the Company and each director, officer, employee, or agent that engages with a potential customer **must verify and record the name and address** of the individual presenting the transaction before providing the individual with any services.

PlanetShop will obtain, or attempt to obtain, the following information from the customer in connection with the reportable transaction.

- The name and address, phone number, date of birth, and driver's license number of the individual presenting the transaction;
- Verification of the identity, of any person or entity on whose behalf the reportable transaction is to be affected by cross referencing the driver's license with the transaction photo.

If the individual is an alien or is not a resident of the United States, the Company MUST examine and record the individual's passport, alien identification card, or other official document evidencing nationality or residence.

3. Where to File CTRs.

The Company will file CTRs with FinCEN through the BSA E-filer system.

4. Retention of CTRs.

The Company shall maintain a copy of each CTR for **at least five (5) years** from the date of the report.

5. Confidentiality of CTRs.

The Company will not inform a customer that it has filed a CTR with regards to the customer's transaction. *See Rules:* 31 C.F.R. §§ 1022.310, 1010.306, 1010.311, 1010.313, and 1010.315.

D. Structuring

Structuring is the practice of conducting financial transactions in a specific pattern calculated to avoid the creation of records and reports pursuant to the BSA.

A person structures a transaction when that person (acting alone or in conjunction with or on behalf of other persons) conducts or attempts to conduct one or more transactions in currency, in any amount, at one or more financial institutions, on one or more days, in any manner, for the

purpose of avoiding the reporting requirements of the BSA (i.e. CTRs, SARs, etc.). An example of structuring is when a person breaks down a transaction of a single sum of currency exceeding $10,000.00 into smaller sums to avoid the filing of a CTR.

Structuring, attempting to structure, or assisting in structuring are illegal and those found guilty of structuring are subject to a fine and imprisonment of up to five (5) years in non-aggravated offenses.

Each director, officer, employee, or agent of the Company is aware that it is illegal to assist any person with structuring. Employees should be alert that attempts by customers to convince them to allow structuring that allows employees to avoid reporting and recordkeeping procedures. *See Rules*: Internal Revenue Manual 4.26.13.1 (Jan. 7, 2016); 31 C.F.R. §§ 1010.100(xx) and 1010.314, 31 U.S.C. § 5324.

E. Registration as Money Services Business

The Company is a registered money services business with FinCEN. The Company must file with FinCEN for a renewal of its registration every year on or before December 31. The CCO will file the renewal documents on behalf of the Company.

An MSB must retain a copy of the submitted registration form and the assigned registration number. If any of the information provided for registration changes, it must be amended with FinCEN.

Registration Number: 31000189227911
Registration Date: May 10, 2021

See Rule: 31 C.F.R. § 1022.380.

F. Law Enforcement Notification

In situations that require immediate attention, such as suspected terrorist financing or ongoing money laundering schemes, PlanetShop will call an appropriate law enforcement authority in addition to filing a SAR-MSB. PlanetShop may call FinCEN's Financial Institutions Hotline at 1-866-556-3974 in addition to filing a timely SAR-MSB.

PlanetShop will comply with the information sharing requirements in FinCEN regulations at 31 C.F.R. *§* 1010.500 *et seq*. These rules specify circumstances in which FinCEN will request information regarding transactions from PlanetShop. In the event PlanetShop receives such a request, PlanetShop will respond to the request and cooperate fully with FinCEN's inquiry. The FinCEN regulations also describe circumstances in which companies may share transaction information with one another, subject to a requirement to provide FinCEN with prior notice. PlanetShop will consult with counsel prior to engaging in information sharing with other companies.

G. Record Retention

All of these records must be retained for five years and must be accessible within a reasonable period of time.

Senior management and the Chief Compliance Officer have approved this Anti-Money Laundering compliance program in writing as reasonably designed to achieve and monitor PlanetShop's ongoing compliance with the requirements of the Bank Secrecy Act and the implementing regulations under it. This approval is indicated by the signature(s) below:

Alexander Spayev

s/Alexander Spayev
Title: Senior Manager

Keren Tamara Gordon

s/Keren Tamara Gordon
Title: Chief Compliance Officer