Green Leaf Business Solutions
AML/BSA Program

Table of Contents

GLBS Table of Contents (cont'd)
AML/BSA Program

20 New Account Policies and Procedures Non High Risk Accounts
Payroll / HRIS Employer Application & Agreement
EMPLOYEE AUTHORIZATION AGREEMENT for payroll direct deposit
Client ACH Authorization

21 Additional Forms for MRB accounts
Addendum to Employer Service Agreement
Partner vendor Information Form

22 Onboarding Due Diligence Summary and Details
Reference information FIN-2014-G001
Payment Express Auto Charge/Auto EFT Enrollment form - TR2 North

23 Required Documents Checklists

Anti-money Laundering Program Background and Green Leaf Business Solutions' Commitment

It is the policy of Green Leaf Business Solutions' 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 the Bank Secrecy Act (BSA) and its implementing regulations.

Money Laundering Defined

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. 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, traveler's checks, cashier'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 funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and 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 require large sums of money and the associated transactions may not be complex.

Regulators have deemed money laundering to include any of the following types of activities:

- Engaging in financial transactions involving funds derived from criminal activities (narcotics trafficking, income tax evasion, fraud, embezzlement, bribery, market manipulation or insider trading, etc.).
- Engaging in financial transactions in furtherance of criminal activity (terrorism, etc.).
- Engaging in any activity designed to prevent detection of the fact that the funds were derived from criminal activity.
- Structuring, or participating in structuring, of transactions to evade money laundering reporting requirements.

The AML/BSA Program

GLBS's Anti-money Laundering (AML/BSA) Program is designed to ensure compliance with all applicable BSA regulations and other related Self-Regulatory Organization and Treasury regulations, and where applicable, relevant rules of the bank regulatory agencies. The program 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.

The AML/BSA Program is also designed to ensure compliance with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) including Section 352 which requires the program to include the following elements:

- Development of internal policies and procedures.
- Appointment of an AML/BSA Compliance Officer.
- Ongoing training.
- Implementation of an Independent Audit function to test AML/BSA Program

GLBS's AML/BSA Program is based on an assessment of risk associated with GLBS's customers, structure, size, products and services, sales force, distribution channels, payroll practices and other relevant factors. Risks are periodically reassessed, and the AML/BSA Program is updated if necessary.

The Importance of an AML/BSA Program for GLBS

Federal law prohibits financial institutions from knowingly engaging in, or assisting with, money laundering activities. This concept of "knowledge" is extremely broad and a financial institution can be guilty of money laundering if it intentionally ignores certain suspicious activities. In addition to detecting and deterring money laundering activities, financial institutions also have a duty to report suspicious activities to the federal government.

Financial institutions and their associates are vulnerable to attempts by criminals to launder money. If such activities occur and GLBS determines that GLBS or its associates knowingly participated in such activities, GLBS and/or the associate may be guilty of money laundering. Although money laundering is usually associated with cash, it is not a required component in a transaction. Any financial transaction may be part of a process to obscure the origin of illegal funds. Day-to-day activities of GLBS associates can, theoretically, be part of a money laundering scheme including opening an account, processing payroll, and processing transactions such as wire transfers and check withdrawals.

Therefore, GLBS associates need to understand what money laundering is, their role in identifying and combating it, and how to apply the policies and procedures of GLBS's AML/BSA Program to their jobs. Failure to comply could result in significant criminal, civil and disciplinary penalties including:

- Fines up to twice the amount of the transaction up to $1 million.
- Employees of financial institutions can be fined individually and sentenced to up to 20 year of imprisonment for knowing or being willfully blind to the fact the transaction involved illegal funds.

Covered Products

Products included in the GLBS AML/BSA Program (covered products) are:

- Payroll Services.
- Benefits Administration
- Full Payroll Tax Support & Limited Payroll Tax Support

Products excluded from the GLBS AML/BSA Program are:

- Time & Attendance
- Applicant Tracking
- Performance Management

Covered Entities

The AML/BSA Program for GLBS is also the AML/BSA Program for Infinity Green Leaf Business Solutions', LLC. Hereafter, when the term GLBS is used, it is inclusive of Infinity Green Leaf Business Solutions', LLC.

Other GLBS subsidiaries or affiliates may be responsible for the design, implementation and administration of AML/BSA programs for their entity's risks. GLBS will work with each of the subsidiaries providing guidance in developing, maintaining and monitoring those AML/BSA programs.

Definition of Terms

The following terms and their definitions are used throughout this AML/BSA Program:

Customer shall include but is not limited to client or accountholder.

- ✓ Associate shall include all employees of GLBS.
- ✓ Account shall include but is not limited to all clients of GLBS.
- ✓ Transaction shall include but is not limited to deposits of money to pay payroll, deposits of contributions, withdrawals or liquidations of funds from an account, or other monetary activities related to an account, policy or contract.

2. Designation of AML/BSA Compliance Officer

(INSERT NAME OF AML/BSA Program Officer) is the company's designated AML/BSA Compliance Officer. The AML/BSA Officer has working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training and has full responsibility and authority to enforce GLBS's AML/BSA Program.

He/She may delegate the role and responsibilities of the AML/BSA Compliance Officer to the Owner, other appointed Compliance Manager or other qualified designee.

The GLBS AML/BSA Compliance Officer shall:

- Monitor GLBS's compliance with AML/BSA obligations.
- Oversee the implementation of new AML/BSA requirements or changes to existing AML/BSA requirements.
- Ensure that appropriate Suspicious Activity Reports (SARs) are filed by (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) with FinCEN when appropriate.
- Ensure all required AML/BSA records are maintained.
- Provide periodic updates to the owner, or any other appointed Chief Compliance Officer regarding the AML/BSA Program.
- Oversee the delivery of AML/BSA communications and training to associates.
- Interact with designated AML/BSA Compliance Officers for subsidiaries.

3. Information Sharing with Government Agencies and Other Financial Institutions
Financial Institutions

Section 314 of the USA Patriot Act is intended to facilitate the sharing of information between governmental entities and financial institutions (314(a)) and between financial institutions themselves (314(b)). The purpose of this sharing is to identify, prevent and deter money laundering and terrorist activity.

The USA Patriot Act provides that sharing information with government agencies and other financial institutions under 314(a) and (b) "shall not constitute a violation" of the privacy provisions of the Gramm-Leach-Bliley Act.

Information Sharing with Government Agencies – Section 314(a)
GLBS will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (314(a) Request) by searching its records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with, each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure website. Unless otherwise stated in the 314(a) Request or specified by FinCEN, GLBS will search those documents outlined in FinCEN's FAQ. If GLBS finds a match, it will be reported to FinCEN via FinCEN's web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (e.g., if FinCEN limits the search to a geographic location), GLBS will structure the search accordingly.

GLBS will respond to 314(a) Requests within 14 days from the transmission date of the request (unless otherwise specified by FinCEN).

If GLBS searches its records and does not find a matching account or transaction, then it will not reply to the 314(a) Request. GLBS will maintain documentation that the required search has been performed. Such documentation will be maintained in the GLBS secure data storage system which will maintain a log of the number of accounts searched and whether a match was found.

GLBS will not disclose the fact that FinCEN has requested or obtained information, except to the extent necessary to comply with the information request. GLBS will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

GLBS will direct any questions regarding the 314(a) Request to the requesting federal law enforcement agency as designated in the request.

Unless otherwise stated in the 314(a) Request, GLBS will not be required to treat the information request as continuing in nature and will not be required to treat the periodic 314(a) Requests as a government-provided list of suspected terrorists for purposes of the customer identification and verification requirements.

Voluntary Information Sharing with Other Financial Institutions – Section 314(b)

GLBS may share information regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering.

Prior to sharing information and annually thereafter, the GLBS Compliance Department (Corporate Compliance) will oversee the filing of the "Notification for Purposes of Section 314(b) of the USA Patriot Act and 31 CFR 1025.540" for GLBS.

Before GLBS shares information with another financial institution, GLBS will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. GLBS understands that this requirement applies even to financial institutions with which we are affiliated and that we will obtain the requisite notices from affiliates and follow all required procedures. Requests for information sharing from a financial institution that is not affiliated with GLBS should be referred to the AML/BSA Compliance Officer.

GLBS will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from GLBS's other books and records.

GLBS will also employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- Identifying and, where appropriate, reporting on money laundering or terrorist activities.
- Determining whether to establish or maintain an account, or to engage in a transaction.
- Assisting the financial institution in complying with performing such activities.

Joint Filing of SARs by Other Financial Institutions

GLBS will file a joint SAR if GLBS and another financial institution that is subject to the SAR regulations are involved in the same suspicious transaction. For example, GLBS and North Bay Credit Union ((INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY)) may file one SAR with respect to suspicious activity payroll services. If a joint SAR is filed, GLBS will maintain a copy of the SAR and supporting documentation in accordance with BSA recordkeeping requirements.

If GLBS determines it is appropriate to jointly file a SAR, we understand that we cannot disclose that we have filed a SAR to any financial institution except the financial institution that is filing jointly. If we determine it is not appropriate to file jointly, we understand that we cannot disclose that we have filed a SAR to any other financial institution.

4. Comparison with Government Lists

Comparison with the Office of Foreign Assets Control's SDN Lists

GLBS will check to ensure that none of its customers appear on the SDN list and are not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by the Office of Foreign Assets Control (OFAC). Generally, GLBS will scan the customer against the SDN list prior to opening an account and quarterly thereafter.

GLBS will access the SDN list through a contracted relationship with a data provider which has such information. As of September, 2019 this will be done in unison with the services of TR2 North LLC.

Because the SDN list and listings of economic sanctions and embargoes are updated frequently, GLBS will request TR2 North to provide and GLBS receive available updates when they occur.

GLBS may rely on the performance of OFAC scans by a vendor or another financial institution before an account is opened when such reliance is reasonable under the circumstances.

If GLBS determines that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, GLBS will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. GLBS will also call the OFAC Hotline at 1-800-540-6322 or use OFAC's e-hotline.

Comparison with Government-provided Lists of Terrorists

At such time as GLBS receives notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for Customer Identification Program purposes, GLBS will, within a reasonable period after an account is opened (or earlier if required by another federal law, regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with federal functional regulators. GLBS will follow all federal directives issued in connection with such lists.

GLBS will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

5. Know Your Customer

Customer Due Diligence
Customer Due Diligence (CDD) and Enhanced Due Diligence are the foundation of a strong AML/BSA compliance program. GLBS performs CDD as part of the underwriting and suitability review processes for new accounts.

At a minimum, GLBS collects the following information:

- The purpose of the account.
- The source of funds and wealth.
- The beneficial owners of the accounts.
- The customer's occupation or type of business.

Based on this information, GLBS can determine the customer's anticipated account activity including volume and type of transactions.

The CDD information is reviewed in connection with, and will provide a baseline for, evaluating customer transactions to determine whether the transactions are suspicious and need to be reported.

For all Managers, Owners, and Financially Interested parties, GLBS will request TR2 North to perform enhanced due diligence. Additional circumstances include, but are not limited to, identification of red flags, requests for contracts in excess of established limits and instances in which the customer does not match the target market for a product.

Customer Identification Program

GLBS's affiliated compliance provider, TR2 North, LLC (TR2N) has implemented a Customer Identification Program for GLBS. For all new accounts the following is performed:

- Verify the identity of their customers who open new accounts.

- Maintain records of information used to verify the customer's identity, including name, address, and other identifying information.
- Determine whether the person seeking to open an account appears on any government lists of known or suspected terrorist organizations.
- Provide notice to customers before an account is opened that information will be collected about them in order to verify their identities.

If a potential or existing customer either refuses to provide the requested customer information when requested, or appears to have intentionally provided misleading information, SFS will not open a new account and, after considering the risks involved, consider closing any existing account for the customer. In either case, our AML/BSA Compliance officer will be notified so that a determination can be made as to whether the situation should be reported to FinCEN (i.e., file a SAR).

If GLBS or TR2N is unable to verify the customer's identification, TR2N will use non-documentary means to verify the customer's identity including:
The primary non-documentary method used will be to run the customer's number from his or her identification document through an independent verification database. If no match is found or other 'red flags' that signal possible money laundering or terrorist financing exist, additional nondocumentary methods may be used to verify a customer's identity such as:

- Contacting the customers.
- Checking references with other financial institutions.
- Obtaining a financial statement.

All affiliates of Green Leaf Business Solutions' are also required to implement a Customer Identification Program that meets the same minimum requirements.

In addition, GLBS verifies the identity of new account owners in the event an existing customer requests to change ownership of a contract.

6. Suspicious Activity Monitoring

The detection and reporting of suspicious activity are keys to the deterrence of money laundering and terrorist activity.

GLBS monitors account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. Monitoring is conducted by associates in the business units manually reviewing transactions for suspicious customer behavior and transaction activity, including but not limited to, examples of money laundering red flag activity provided in Exhibit A. An associate who detects suspicious activity will bring it to the attention of his or her supervisor who will consult with the AML/BSA Compliance Officer.

The AML/BSA Compliance Officer will conduct reviews of potentially suspicious activity detected by the business units. The AML/BSA Compliance Officer will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR is filed.
Relevant information can include, but not be limited to, the following: banking information, source of funds verification, financial/estate planning documentation and business information.

The AML/BSA Compliance Officer or his/her designee is responsible for monitoring the business unit's review of any activity that is detected as possibly suspicious. The AML/BSA Compliance Officer will also determine whether additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

Emergency Notification to the Government by Telephone
Certain suspicious activities require immediate telephone reporting of the transaction. These situations include but are not limited to instances when:

- A customer's name is on the OFAC list.
- A customer tries to use bribery, coercion, or similar means to open an Account or carry out a suspicious activity.
- GLBS has reason to believe a customer is trying to move illicit cash out of the government's reach.
- GLBS has reason to believe a customer is about to use the funds to further an act of terrorism.

GLBS will call one or more of the following:

- OFAC Hotline.
- FinCEN's Department's Financial Institutions Hotline.
- Local United States Attorney's Office.
- Local FBI Office.
- Local SEC Office.

7. Suspicious Activity and BSA Reporting

Suspicious Activity Report Filing

GLBS will report to FinCEN any transaction that, alone or in the aggregate, involves at least $10,000 in funds or other assets, and GLBS knows, suspects, or has reason to suspect that it falls within one of following classes:

- The transaction involves funds derived from illegal activity (MRB) or is intended or conducted to hide or disguise funds or assets derived from illegal activity.
- The transaction is designed, whether through structuring or other means, to evade the requirements of the BSA.

- The transaction appears to serve no business purpose or apparent lawful purpose or is not the sort of transaction in which the particular customer would be expected to engage and for which GLBS knows of no reasonable explanation after examining the available facts.
- The transaction involves the use of GLBS to facilitate criminal activity.

The above guidelines extend to patterns of transactions. Therefore, if GLBS determines that a series of transactions would not independently trigger suspicion, but when taken together, form a suspicious pattern of activity, GLBS will inform (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a SAR. Also, if a transaction doesn't meet a specific dollar threshold that would trigger the filing of (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a SAR, but does raise an identifiable suspicion of criminal, terrorist, or corrupt activities, GLBS will appropriately review the transaction and determine if a SAR should be filed.

GLBS will also inform (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a SAR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes.

GLBS may ask (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a SAR for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported under the SAR rule.

GLBS will report suspicious transactions informing (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a SAR and will collect and maintain supporting documentation as required by the BSA regulations. (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) should will file a SAR no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. If no suspect is identified on the date of the initial detection, we may delay request to have (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) file the SAR for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase "initial detection" does not mean the moment a transaction is identified for review. The 30-day (or 60-day) period begins when an appropriate review is conducted, and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

Generally, GLBS will report any continuing suspicious activity on a previously filed SAR with a new request for (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a SAR at least every 90 days. GLBS will continue to assess whether it should continue to maintain the account or effect the transaction in question.

GLBS will retain copies of any SAR filed by (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) and the original or business record equivalent of any supporting documentation for at least five years from the date of filing the SAR. We will identify and maintain supporting

documentation and make such information available to FinCEN, or any other appropriate law enforcement agencies upon request.

GLBS will not notify any person involved in the transaction that the transaction has been reported, except as permitted by BSA regulations. In the event GLBS is subpoenaed or required to disclose a SAR or the information contained in the SAR, we will decline to produce the SAR and any information that would disclose that an SAR was prepared or filed, except where disclosures are requested by FinCEN, or another appropriate law enforcement or regulatory agency. GLBS will notify FinCEN of any such request and our response.

Exceptions to Filing a Suspicious Activity Report

GLBS is not required to ask (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a SAR to report as the result of:

- A robbery or burglary that is reported by GLBS to appropriate law enforcement authorities.

State Reporting Requirements

Certain states have enacted their own reporting requirements which may or may not be satisfied by reporting to the federal government. Consequently, whenever any type of transaction report under the BSA is filed with the federal government, GLBS will undertake efforts to analyze relevant state law to determine whether a duplicate or comparable form needs to be filed with a state authority.

Safe Harbor Provisions

Federal law provides broad "safe harbor" protection from civil liability for the filing of SARs to report suspected or known criminal violations and suspicious activities, regardless of whether such reporting is mandatory or is done on a purely voluntary basis. The BSA provides that a financial institution and its directors, officers, associates, and agents who file a SAR "shall not be liable to any person" for such disclosure or for any failure to notify the person involved in the transaction or any other person of such disclosure.

Form 8300

GLBS's Monetary Instruments Policy prohibits the receipt of cash and currency as defined in the instructions for Form 8300 reporting. If GLBS discovers such transactions have occurred, GLBS will file a Form 8300 with FinCEN for currency transactions that exceed $10,000. GLBS will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a Form 8300 if the transactions total more than $10,000 and are made by or on behalf of the same person during any one business day.

Although GLBS does not accept currency, cashier's checks are accepted. Cashier's checks in amounts less than $10,000 are tracked. GLBS will file a Form 8300 or ask (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a SAR if we know the payer is trying to avoid the reporting of such a transaction on Form 8300.

Currency and Monetary Instrument Transportation Reports (CMIR)
GLBS's Monetary Instruments Policy prohibits the receipt of currency. GLBS will file a Currency and Monetary Instrument Transportation Report (CMIR) with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the United States, currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time. We will also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal service or by common carrier, currency or other monetary instruments of more than $10,000 at one time.

Report of Foreign Bank and Financial Accounts (FBAR)
GLBS will file a Report of Foreign Bank and Financial Accounts for any financial accounts in a foreign country of more than $10,000 that we hold, or for which we have signature authority over.

Under Treasury's Joint and Travel rule, when GLBS wire transfers funds, GLBS will create a paper trail by which enforcement officials can trace the transfer of such funds. At a minimum, GLBS will record in writing the following information:

- Name and address of the sender and recipient
- Amount of the transmittal
- Identity of recipient's financial institution
- Account number of the recipient
- Date of the transaction

8. AML/BSA Recordkeeping

Responsibility for Required AML/BSA Records and SAR Filings

GLBS's AML/BSA Compliance Officer is responsible for ensuring that the AML/BSA records are maintained properly and that SARs are filed as required by (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY).

In addition, as part of our AML/BSA program, GLBS will maintain all copies of SARs, Form 8300s, CMIRs, FBARs and relevant documentation on funds transmittals. We will maintain SAR and accompanying documentation for at least five years. GLBS will maintain other documents according to existing BSA and other recordkeeping requirements and GLBS's Information Governance Program.

SAR Maintenance and Confidentiality

GLBS will hold SARs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, or other appropriate law enforcement or regulatory agency about a SAR filing. We will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed. GLBS will notify FinCEN of any such subpoena requests that are received. We will segregate SAR filings and copies of supporting documentation from other books and records to avoid disclosing SAR filings. GLBS's AML/BSA Compliance Officer will handle all subpoenas or other requests for SARs. We may share information with another financial institution about suspicious transactions in order to determine whether to file a joint SAR. In cases in which we file a joint SAR for a transaction that has been handled by GLBS and another financial institution, both financial institutions will maintain a copy of the filed SAR.

It is our policy that all SARs will be reported to the Chief Compliance Officer regularly with a clear reminder of the need to maintain the confidentiality of the SAR.

9. Associate Training

The GLBS AML/BSA Program training is developed and maintained under the leadership of the AML/BSA Compliance Officer and/or designee and meets the following requirements:

- Occurs at least annually.
- Is required for all associates with administrative responsibility for covered products.
- Is reviewed and updated as necessary, to reflect new developments in the regulation.
- Documentation evidencing completion of training is maintained in accordance with records retention requirements.
- Is included in the scope of the periodic (commensurate with the risks posed by GLBS's covered products) AML/BSA audit conducted by the Internal Audit Department.

Associates whose job responsibilities require AML/BSA training may include, but are not limited to, associates who open accounts, handle client payroll accounts, checks or wire transfers, or process client transactions, and associates who supervise such associates.

Training Program Content

GLBS's AML/BSA Training Program includes, but is not limited to, information that provides an understanding of money laundering activities, prevention and detection methods, and regulatory requirements.

Basic AML/BSA training content includes:

- How to identify red flags and signs of money laundering that may arise during the course of the employee's duties.
- 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).

- The employees' role in the AML/BSA Compliance program and how to perform them.
- The disciplinary consequences including civil and criminal penalties for noncompliance with the BSA.

The development of AML/BSA training may be delegated to appropriate persons selected by the GLBS AML/BSA Compliance Officer. Specialized content will be identified and may be developed by management of the areas in need of such training.

Training Program Implementation
Training records will be maintained in accordance with the GLBS Records Retention Schedule. Delivery of AML/BSA training may be through on-line industry courses, web-ex, educational pamphlets, videos, intranet systems, in-person lectures, explanatory memos and other methods.

10. Independent Testing

The audit of GLBS's AML/BSA program will be performed periodically, commensurate with the risks posed by GLBS's covered products, by the Internal Audit Department in coordination with the Corporate Compliance Department and may include:

- Evaluating the overall integrity and effectiveness of GLBS's AML/BSA Compliance Program.
- Evaluating GLBS's procedures for BSA reporting and recordkeeping requirements.
- Evaluating internal monitoring program and, if necessary, perform additional testing of GLBS's transactions with an emphasis on high-risk areas.
- Evaluating adequacy of training programs.
- Evaluating process for identifying suspicious activity.
- Evaluating process for reporting suspicious activity.
- Evaluating policy for reviewing accounts that generate multiple SAR filings.
- Evaluating GLBS's response to previously identified deficiencies.

The scope of the audit will be determined by the Internal Audit Department. Audit findings, including recommendations to remedy any deficiencies, will be reported to the GLBS AML/BSA Compliance Officer. The GLBS AML/BSA Compliance Officer will be responsible for evaluating and implementing any recommendations and will have final approval authority over action dates and assignments established in response to Audit Improvement Agreements. The GLBS AML/BSA Compliance Officer will also determine additional distribution of the final audit report.

11. Confidential Reporting of AML/BSA Non-Compliance

GLBS associates will report any violations of GLBS's AML/BSA Program to the AML/BSA Compliance Officer, unless the violations implicate the Compliance Officer, in which case the

associate shall report to the GLBS Chief Compliance Officer or General Counsel. Such reports will be confidential, and the associate will suffer no retaliation for making them.

12. Senior Management Approval of AML/BSA Program

The AML/BSA Compliance Officer has approved the AML/BSA Compliance Program as reasonably designed to achieve and monitor GLBS's ongoing compliance with the requirements of the BSA and its implementing regulations.

The Chief Compliance Officer will be provided a copy of the AML/BSA Program document periodically, at least every three years or upon substantive revision. The AML/BSA Compliance Officer will consider program revisions, if any, as suggested by the Chief Compliance Officer.

13. Money Laundering Red Flags

Certain red flags may signal possible money laundering or terrorist financing activities. The following list of money laundering and terrorist financing red flags may be noted at the point of sale or while processing a transaction. Their presence may indicate the need to notify the GLBS AML/BSA Compliance Officer to determine if the situation warrants further investigation and possible filing of a SAR by (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY).

Customer Identity Red Flags

- Legal entity is known to be associated with a terrorist organization or conducts business in a jurisdiction that has been designated by the U.S. as a primary money laundering concern or has been designated as non-cooperative by an international body.
- The customer is from or has accounts in a country identified as a non-cooperative country or territory.
- There is overlap between corporate officers or other identifiable similarities associated with addresses, references, and anticipated financial activities.
- The customer gives a false or stolen SSN.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

Reason for Opening the Account Red Flags

- The customer exhibits unusual concern about GLBS's compliance with government reporting requirements and GLBS's AML/BSA policies (particularly concerning his or her identity, types of business and assets), or is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspicious identification or business documents;

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business or investment strategy.
- The occupation stated by the customer is not commensurate with the level or type of potential activity for the account.
- Unexplained inconsistencies of data are noted during the process of identifying or verifying a customer.
- The purpose for opening an account for non-profit or charitable organization appears to have no economic purpose or link between the stated mission of the organization and other parties to the transaction.

Customer Behavior Red Flags

- The customer exhibits a lack of concern regarding risks, commission, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer makes an unusual request, such as asking for help in converting cash into checks.
- The customer is always in a rush.
- The customer requests that the account opening transaction be processed to avoid GLBS's normal documentation requirements.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer seeks to change or cancel a transaction after being informed that a report will be filed or that information will need to be verified.
- The customer conducts its business under unusual circumstances, at irregular hours or in unusual locations.
- The customer offers gifts or gratuities greater than GLBS's policies allow after being informed of GLBS's policies.
- The customer (or someone connected with the account) is the subject of news reports or rumors indicating possible criminal regulatory, or civil fraud violations.
- The customer (or someone connected with the account) is the subject of inquiry or investigation by a regulatory or criminal prosecutorial agency.

Customer Transaction Red Flags

- The customer engages in excessive journal entries between unrelated accounts with no apparent business purpose.
- The customer makes deposits with multiple monetary instruments purchased from the same and/or different financial institutions.

- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- The customer account has unexplained or sudden extensive wire activity, where previously there had been little or no wire activity.
- The customer makes a fund deposit followed by an immediate request that the money be withdrawn or transferred to a third party, or to another business without any apparent business reason.
- The customer's transactions are unusual or inconsistent with the customer's normal trading practices.
- The customer makes investments that do not make economic sense, such as large sums sitting in a money market account.

Source of Funds Red Flags

- Unexplained or negotiation of third-party checks.
- The source of funds is suspicious such as transfers from a bank or other type of account that do not appear to have a legitimate relationship with the business.
- The customer's source of funds or other assets appear to be well beyond the resources of the person or entity.
- The information provided by the customer that identifies legitimate sources for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for funds and other assets.

FinCen Specific Red Flags for MRB Accounts

- A customer appears to be using a state-licensed marijuana-related business as a front or pretext to launder money derived from other criminal activity (i.e., not related to marijuana) or derived from marijuana-related activity not permitted under state law.
- The business receives substantially more revenue than may reasonably be expected given the relevant limitations imposed by the state in which it operates.
- The business receives substantially more revenue than its local competitors or than might be expected given the population demographics.
- The business is depositing more cash than is commensurate with the amount of marijuana-related revenue it is reporting for federal and state tax purposes.
- The business is unable to demonstrate that its revenue is derived exclusively from the sale of marijuana in compliance with state law, as opposed to revenue derived from (i) the sale of other illicit drugs, (ii) the sale of marijuana not in compliance with state law, or (iii) other illegal activity.
- The business makes cash deposits or withdrawals over a short period of time that are excessive relative to local competitors or the expected activity of the business.
- Deposits apparently structured to avoid Currency Transaction Report ("CTR") requirements.
- Rapid movement of funds, such as cash deposits followed by immediate cash withdrawals.
- Deposits by third parties with no apparent connection to the accountholder.
- Excessive commingling of funds with the personal account of the business's owner(s) or manager(s), or with accounts of seemingly unrelated businesses.
- Individuals conducting transactions for the business appear to be acting on behalf of other, undisclosed parties of interest.
- Financial statements provided by the business to the financial institution are inconsistent with actual account activity.
- A surge in activity by third parties offering goods or services to marijuana-related businesses, such as equipment suppliers or shipping servicers.
- The business is unable to produce satisfactory documentation or evidence to demonstrate that it is duly licensed and operating consistently with state law.
- The business is unable to demonstrate the legitimate source of significant outside investments.
- A customer seeks to conceal or disguise involvement in marijuana-related business activity. For example, the customer may be using a business with a non-descript name (e.g., a "consulting," "holding," or "management" company) that purports to engage in commercial activity unrelated to marijuana, but is depositing cash that smells like marijuana.
- Review of publicly available sources and databases about the business, its owner(s), manager(s), or other related parties, reveal negative information, such as a criminal record, involvement in the illegal purchase or sale of drugs, violence, or other potential connections to illicit activity.

- The business, its owner(s), manager(s), or other related parties are, or have been, subject to an enforcement action by the state or local authorities responsible for administering or enforcing marijuana-related laws or regulations.
- A marijuana-related business engages in international or interstate activity, including by receiving cash deposits from locations outside the state in which the business operates, making or receiving frequent or large interstate transfers, or otherwise transacting with persons or entities located in different states or countries.
- The owner(s) or manager(s) of a marijuana-related business reside outside the state in which the business is located.
- A marijuana-related business is located on federal property or the marijuana sold by the business was grown on federal property.
- A marijuana-related business's proximity to a school is not compliant with state law.
- A marijuana-related business purporting to be a "non-profit" is engaged in commercial activity inconsistent with that classification, or is making excessive payments to its manager(s) or employee(s).

Company Name:	Green Leaf Business Solutions
SOP Name:	New Client Lead Type Determination
Purpose:	The purpose of this SOP is to determine what type of client is being onboarded into the system.
Policy:	This policy is in place to make sure that the correct type of client onboarding is performed based on the correct type of checks and balances in place for each type of client that is on-boarded.
Scope:	New Client Intake Department
Employee Responsible:	(INSERT EMPLOYEE NAME OR ROLE OF RESPONSIBLE)
Definitions:	**Partner referrals-** A partner referral is any new business that is referred from Back of the House and AOC. **Warm lead**- A warm lead is a referral from a CPA or broker or a new business for an existing client. **Cold Lead**- A cold lead comes from a marketing campaign, a sales account executive cold calling a business or a business that calls us. **Back of The House-** (Insert definition of) **AOC**-(Insert definition of) **CPA-** A CPA is a Certified Public Accountant. **Broker**-(Insert definition of) **New Business for existing client-** (Insert definition of) **Marketing campaign-**(Insert definition of) **Sales Account Executive cold calling a business-**(Insert definition of) **Business that calls us-**(Insert definition of)
Resources:	N/A
Effective Date:	SEPT 2019

New Client Lead Type Determination

1. Determine which source referred over the lead.

a. "Back of The House"
b. "AOC"
c. "CPA"
d. "Broker"
e. "New Business for existing client"
f. "Marketing campaign"
g. "Sales Account Executive cold calling a business"
h. "Business that calls us"

A. If "Back of the house"
Then it is classified as a Partner referral
Please follow SOP Titled Partner referrals

B. If "AOC"
Then it is classified as a Partner referral
Please follow SOP Titled Partner referrals

C. If "CPA"
Then it is classified as a Warm lead
Please follow SOP Titled Warm Leads

D. If "Broker"
Then it is classified as a Warm lead
Please follow SOP titled Warm Leads

E. If "New Business for existing client"
Then it is classified as a Warm lead
Please follow SOP titled Warm leads

F. If "Marketing campaign"
Then it is classified as a Cold lead
Please follow SOP titled Cold leads

G. If "Sales Account Executive cold calling a business"
Then it is classified as a Cold lead
Please follow SOP titled Cold leads

H. If "Business that calls us"
Then it is classified as a Cold lead
Please follow SOP tilted Cold leads

Company Name:	Green Leaf Business Solutions
SOP Name:	COLD LEADS
Purpose:	The purpose of this SOP is to give the processes and procedures on how to handle the verification of a Cold Lead at inception. This can only be performed after following SOP "New Client Lead Type Determination".
Policy:	This policy is in place to make sure that the correct type of client onboarding and vetting is performed after SOP "New Client Lead Type Determination" has been performed.
Scope:	Sales Department, Implementation Department
Employee Responsible:	Sales Rep, Implementation Employee
Definitions:	**Cold Lead**- A cold lead comes from a marketing campaign, a sales account executive cold calling a business or a business that calls us. **Tax Service-**(Insert definition of) **Direct Deposit**-(Insert definition of) **Payrol**l-(Insert definition of) **Checks Only**-(Insert definition of) **Onsite Check -**Sales rep meets the client at their place of business **Hand Off Sheet-** (Insert definition of) **Social Network Search-** (Insert definition of) **Business Website Review-** (Insert definition of) **Equifax check-(** Insert definition of) **M drive implementation folder-(** Insert definition of) **OFAC search-(** Insert definition of)
Resources:	Computer with Access to Wifi, The Hand off Sheet, Equifax pull ability, access to M Drive, OFAC Search capability in Equifax
Effective Date:	Sept 2019

COLD LEADS

All clients that come to us via a cold lead cannot have direct deposit for their first payroll (checks only) and must be on tax service.

Steps:

1. **Sales department does;**
    - Onsite Check (meets the client at their place of business) and,
    - Documents who they met with,
    - The address and the date.
    - This needs to be added to the hand off sheet and must include fields for;
        - Address
        - Who they met,
        - Date and
        - Sales person signature

2. **Sales department can do either this option listed above in #1 or the Google search** Google Search;
        - Sales department runs a Google search of business and business location.
        - The screenshots of the search results will be sent as an attachment with all the other paperwork submitted to implemenation@payroll-us.com.

3. **Sales department requests a copy of the business owner's driver license.** To be included as an attachment with all the other paperwork submitted to (insert implementation dept email)

4. **Sales department does a social network search on owners** – The screenshots of the search results will be sent as an attachment with all the other paperwork submitted to (insert implementation dept email)

5. **Sales department does a business website review** – The screenshots of the search results will be sent as an attachment with all the other paperwork submitted to implemenation@payroll-us.com.

6. **Implementation runs an;**

    - **Equifax check on client and,**
    - **saves the document to the M drive implementation folder**

7. **Implementation runs an OFAC search** – this will appear on the Equifax summary

Company Name:	Green Leaf Business Solutions
SOP Name:	PARTNER REFERRAL
Purpose:	The purpose of this SOP is to give the processes and procedures on how to handle the verification of a Partner Referral at inception. This can only be performed after following SOP "New Client Lead Type Determination".
Policy:	This policy is in place to make sure that the correct type of client onboarding and vetting is performed after SOP "New Client Lead Type Determination" has been performed.
Scope:	Sales Department, Implementation Department
Employee Responsible:	Sales Rep, Implementation Employee
Definitions:	**Partner Referral** - A partner referral is any new business that is referred from Back of the House and AOC **Equifax check-(** Insert definition of) **M drive implementation folder-(** Insert definition of) **OFAC search-(** Insert definition of)
Resources:	Computer with Access to Wifi, Equifax pull ability, access to M Drive, OFAC Search capability in Equifax
Effective Date:	Sept 2019

PARTNER REFERRAL

Steps:

1. **Sales department does a <u>Google Search;</u>**
    - Sales department runs a Google search of business and business location.
    - The screenshots of the search results will be sent as an attachment with all the other paperwork submitted to implemenation@payroll-us.com.

2. **Implementation runs an;**
    - **<u>Equifax check</u> on client and,**
    - **saves the document to the <u>M drive implementation folder</u>**

3. **Implementation runs an <u>OFAC search</u>** – this will appear on the Equifax summary

Company Name:	Green Leaf Business Solutions
SOP Name:	WARM LEADS
Purpose:	The purpose of this SOP is to give the processes and procedures on how to handle the verification of a Warm lead at inception. This can only be performed after following SOP "New Client Lead Type Determination".
Policy:	This policy is in place to make sure that the correct type of client onboarding and vetting is performed after SOP "New Client Lead Type Determination" has been performed.
Scope:	Sales Department, Implementation Department
Employee Responsible:	Sales Rep, Implementation Employee
Definitions:	**Warm Lead**- A warm lead is a referral from a CPA or broker or a new business for an existing client **Onsite Check -**Sales rep meets the client at their place of business **Hand Off Sheet-** (Insert definition of) **Equifax check-(** Insert definition of) **M drive implementation folder-(** Insert definition of) **OFAC search-(** Insert definition of)
Resources:	Computer with Access to Wifi, The Hand off Sheet, Equifax pull ability, access to M Drive, OFAC Search capability in Equifax
Effective Date:	Sept 2019

WARM LEADS

Steps:

1. **Sales department does;**
    - Onsite Check (meets the client at their place of business) and,
    - Documents who they met with,
    - The address and the date.
    - This needs to be added to the hand off sheet and must include fields for;
        - Address
        - Who they met,
        - Date and
        - Sales person signature

2. **Sales department can do either this option listed above in #1 or the Google search**
   Google Search:
        - Sales department runs a Google search of business and business location.
        - The screenshots of the search results will be sent as an attachment with all the other paperwork submitted to implemenation@payroll-us.com.

8. **Sales department requests a copy of the business owner's driver license.** To be included as an attachment with all the other paperwork submitted to (insert implementation dept email)

3. **Implementation runs an;**
    - **Equifax check on client and,**
    - **saves the document to the M drive implementation folder**

4. **Implementation runs an OFAC search** – this will appear on the Equifax summary

New Business onboarding
High-Risk Business Form

Name of Rep Filling this form out: _____
Date: _____
Name of Business: _____
Primary Business activity: _____

Determine if the business is a high-risk business by following normal onboarding protocols. If the protocol results in the business being any of the following below, please fill this form out as well as the "**Marijuana Related Business Worksheet".**

Is the business engaged in any of the following?

- ☐ Marijuana related Businesses (Please also fill out the "Marijuana Related Business Worksheet" along with this form)
- ☐ Casinos and card clubs.
- ☐ Offshore corporations and banks located in tax and/or secrecy havens.
- ☐ Leather goods stores.
- ☐ Car, boat, and plane dealerships.
- ☐ Used automobile or truck dealers and machine parts manufacturers.
- ☐ Travel agencies.
- ☐ Brokers/dealers.
- ☐ Jewel, gem, and precious metal dealers.
- ☐ Import/export companies.
- ☐ Auctioneers.
- ☐ Deposit brokers.
- ☐ Pawn brokers.
- ☐ Ship, bus, and plane operators.
- ☐ Telemarketers.
- ☐ Pornography websites or adult entertainment services of any sort.
- ☐ Other high-risk business not listed. Insert type here:

If YES to any of the above, then refer to the onboarding manual for high risk businesses. As well, please turn this form into (INSERT NAME OF AML/BSA Program Officer and email) after filling out as a high-risk business.

Marijuana Related Business Worksheet
(MRB Determination Form)

Tier 1

- ☐ Marijuana dispensaries
- ☐ Marijuana cultivation (growers)
- ☐ Marijuana oil (THC and CBD) extractors
- ☐ Marijuana infused product producers (edibles)
- ☐ Cannabis seeds
- ☐ Processing
- ☐ Testing
- ☐ Retail delivery
- ☐ Planting
- ☐ Packaging
- ☐ Transporting
- ☐ Cannabidiol

Tier 2

- ☐ Sellers of products related to growing marijuana (lights, watering systems, fertilizer)
- ☐ Sellers of products for consuming marijuana (vape pens and cartridges, pipes, bongs)
- ☐ Industry associations
- ☐ Payroll providers
- ☐ Advertising and media providers
- ☐ Some software providers
- ☐ Hydroponic supplies
- ☐ Payment processors
- ☐ Packaging supplies
- ☐ Advertising and public relations
- ☐ Industry associations
- ☐ Marijuana software

Tier 3

- ☐ Attorneys
- ☐ Accountants
- ☐ Registered agents
- ☐ Commercial property owners
- ☐ Compliance consultants
- ☐ Training and education providers
- ☐ Some software and technology providers

**Please explain in a few short sentences, why you feel the new business fits into the category selected?

_____

Name of Employee filling out this form:_____
Date:_____

(After done filling this out. Please send to (INSERT NAME OF AML/BSA Program Officer) (INSERT NAME OF AML/BSA Program Officer and email) ***as soon as possible. Make sure she confirms receipt.)***

Instructions when filing out the "**Marijuana Related Business Worksheet**"

If Marijuana Related Business (MRB) , here is helpful guide to help determine which Tier the business falls under.

Tier 1 MRBs are considered the riskiest because they literally touch marijuana at some point along the supply chain and most clearly "manufacture, distribute, or dispense marijuana."6 Tier I MRBs generally encompass businesses licensed by a state or "marijuana-related legitimate business," as defined in proposed federal marijuana banking bills.

Tier II MRBs are considered less risky than Tier I MRBs because they do not directly "manufacture, distribute, or dispense marijuana" and are typically not licensed by a state as a "marijuana business" per se. However, Tier II MRBs are considered "marijuana businesses" within the framework because they are specifically focused on providing pro-ducts and services to Tier I MRBs and the marijuana industry in general. The majority, if not all, of a Tier II MRB's revenue might reasonably be expected to come from Tier I MRBs and marijuana related activities. Therefore, Tier II MRBs might be considered to be "aiding and abetting" the more clearly defined and federally illegal Tier I MRBs. Tier II MRBs are sometimes referred to as "ancillary" or "indirect" MRBs as opposed to "direct" Tier I MRBs.
In Summary: Businesses that are still considered marijuana businesses but are typically not a state-licensed marijuana business because they don't touch the plant. These businesses are specifically focused on providing products and services to Tier I MRBs.

Tier III MRBs are considered the least risky tier and not a "marijuana businesses" in the strictest sense. Unlike Tier II MRBs, Tier III MRBs are not specifically focused on selling to Tier I MRBs or the marijuana industry. In addition, selling to Tier I MRBs is incidental to a Tier III MRB's overall business and revenue. However, Tier III MRBs are specific businesses known to serve Tier I MRBs and, as such, might still be considered to be "aiding and abetting" an illegal activity in a strict sense. Tier III MRBs can be any type of business, but generally include professional services firms;

(The rest of this page left intentionally Blank)

List of emails, templates, and forms utilized in Onboarding DD Process

1. “Policies and Procedures for High Risk Accounts (NON-MRBs)”
2. “MRB Welcome email”
3. “Regular account documents and contracts” (if not previously provided)
4. “Addendum to Service Agreement”
5. “Request for Additional info form”
6. “Enhanced Background Check (EBC)”
7. “EBC Report”
8. “Application Denied email”
9. “Info requested per EBC”
10. “EBC Passed, Additional Info required email”
11. “EBC passed documents required form”
12. “2nd site visit scheduled for a last chance effort”
13. “Additional time frame granted under probationary period”
14. “Final decline letter”
15. “Final approval email”.

Policies and Procedures for High Risk Account (HRA)

1.
Compliance Manager to have discussion with Marc Rodriguez to decide if they want to proceed to take on the account HRA (High Risk Account).

2A.
If Yes, then proceed to Step 3.

2B.
If No, then send out **"Letter of decline for HRA"** via certified mail.

3.
Have a call with True North to discuss the licensing and additional custom document types the HRA must submit in order for Green Leaf Business Solutions to be in compliance with CDD policies.

4.
Send out email titled **"HRA Additional info request"**

Attachments:

1. "**HRA Addendum to contract**" (True North to provide)
2. "**HRA List of requested additional documents"** (True North to provide)

5. After documents are returned, Upload returned documents to the teamwork portal under client profile.

6. True North to run **"Enhanced Background Check (EBC)"** and upload findings with a **"EBC Report"** into teamwork portal.

7A. If NO negative findings, proceed to open account.
7B. If YES negative findings, hold a call with True North to discuss next steps and create a **"Custom HRA Plan"** to handle this new type of HRA.

8. Take action based on custom next steps plan outlined between Green Leaf Business Solutions and True North.

9. Add that plan as an addendum to this set of policies and procedures.

Forms, email and documents mentioned

1. **“Letter of Decline for HRA”**
2. **“Enhanced Background Check (EBC)”**
3. **“EBC Report”**

<u>Custom TBD Forms:</u>

1. **“HRA Additional info request”**
2. “**HRA Addendum to contract**”
3. “**HRA List of requested additional documents”**
4. **“Custom HRA plan”**

Green Leaf Business Solutions Policies and Procedures for CDD, AML, BSA Program

(Based on "FIN-2014-G001 Issued: February 14, 2014
Subject: BSA Expectations Regarding Marijuana-Related Businesses")

"GLBS" will at application and periodically throughout the year check for the "Cole Memo priorities"

Below each bulleted Cole memo, is the way in "GLBS" will check for these guidelines as marked in (___) and italicized.

- Preventing the distribution of marijuana to minors
  (Site checks results)

- Preventing revenue from the sale of marijuana from going to criminal enterprises, gangs, and cartels
  (Reviewing bank statements)

- Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
  (Site Checks and Bank Statements reviews)

- Preventing state-authorized marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
  (Through interview questions, and site checks)

- Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
  (Site Checks)

- Preventing drugged driving and the exacerbation of other adverse public health consequences associated with marijuana use;
  (Enhanced background checks, Site checks)

- Preventing the growing of marijuana on public lands and the attendant public safety and environmental dangers posed by marijuana production on public lands; and
  (Site checks, google earth checks, enhanced background checks)

- Preventing marijuana possession or use on federal property.
  (Site checks, google earth checks, enhanced background checks)

Policies and Procedures on Assessing Risk, Performing CDD While Providing Payroll to Marijuana-Related Businesses

In assessing the risk of providing services to a marijuana-related business, Green Leaf Business Solutions will conduct customer due diligence that includes:

1. Verifying with the appropriate state authorities whether the business is duly licensed and registered.

"GLBS" Will have True North verify this information as part of their "Enhanced Background Check (EBC)" (Step 4 of Policies and Procedures High Risk MRB)

2. Reviewing the license application (and related documentation) submitted by the business for obtaining a state license to operate its marijuana-related business.

"GLBS" will request a copy of their state license application and have it reviewed by True North. This will be done after the EBC has been passed (Step 4 of Policies and Procedures High Risk MRB)

3. Requesting from state licensing and enforcement authorities available information about the business and related parties.

This is part of Step 4 of Policies and Procedures High Risk MRB

4. Developing an understanding of the normal and expected activity for the business, including the types of products to be sold and the type of customers to be served (e.g., medical versus recreational customers).

This is part of the application process under questions # ___, and #

Question from application:

What types of products do you sell?

What types of customers do you serve?

Medical? Y/N

Recreational? Y/N

Forms:

"Expected Monthly Account Activity form"

"Vendor and Supplier Information"

5. Ongoing monitoring of publicly available sources for adverse information about the business and related parties.

This is part of the daily monitoring service provided by True North. It is Step 14 in the Policies and Procedures High Risk MRB

6. Ongoing monitoring for suspicious activity, including for any of the red flags described in this guidance.

"GLBS" checks for all red flags and warning issued by FinCen and all other sources as part of our monthly review process. Those are part of our "Constant Red Flag Watch List"

7. Refreshing information obtained as part of customer due diligence on a periodic basis and commensurate with the risk.

"GLBS" are provided with, and keep on record;

-Background checks on all new employees.

-Site visits on all new locations.

-EBC on all Owners and Managers (daily)

-Recurring Site visits 2 times per 12 months.

Ongoing training: Compliance Manager will also be taking refresher compliance training every 6 months for updated AML/BSA Training.

8. As part of our CDD we will consider whether a marijuana-related business implicates one of the Cole Memo priorities or violates state law.

"GLBS" will do this by having a Cannabis Compliance Auditor (True North) perform site checks to see compliance with state law. This is done initially within 30 days of services. Again every 6 months thereafter. If there are issues found not to be in compliance with State law, there is a remediation request given to the MRB. They then have 45 days to get these issues resolved. Proof is then turned in. A 2nd site visit may be ordered to run a 2nd site check if warranted to provide evidence of compliance firsthand by a 3rd party auditor. This is all part of the Policies and Procedures for MRBS and listed as steps 7-13.

As well we have a Cannabis Auditor firm (True North) for review of current MRB Standard Operating Procedures, and HR Training Records for checks with State compliance.

9. Filing Suspicious Activity Reports on Marijuana-Related Businesses

"GLBS" is not required to file a SAR, but will notify (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) if "GLBS" knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through "GLBS":

1. Involves funds derived from illegal activity (MRB).

2. Attempt to disguise funds derived from illegal activity.

3. Is designed to evade regulations promulgated under the BSA.

4. Lacks a business or apparent lawful purpose.

10. Green Leaf Business Solutions will file SAR Reports to FinCen.

Types of SAR to be filed by (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY):

1. "Marijuana Limited" SAR Filing

"GLBS" will ask (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a Marijuana Limited SAR when we reasonably believe, based on our customer due diligence, the MRB does not implicate;

- *One of the Cole Memo priorities*
- *Violate state law*

The content of this SAR will be limited to the following information:

- *Identifying information of the subject and related parties;*
- *Addresses of the subject and related parties;*
- *The fact that the filing institution is filing the SAR solely because the subject is engaged in a marijuana-related business; and*
- *The fact that no additional suspicious activity has been identified.*

"(INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY)" will use the term "MARIJUANA LIMITED" in the narrative.

2. "Marijuana Priority" SAR Filings

"GLBS" will ask (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a "Marijuana Priority" SAR on a marijuana-related business that we reasonably believe, based on our customer due diligence, the MRB implicates;

- *One of the Cole Memo priorities or*
- *Violates state law*

The content of this SAR will include comprehensive detail in accordance with existing regulations and guidance.

- *Details particularly relevant to law enforcement in this context include:*
- *Identifying information of the subject and related parties;*

- *Addresses of the subject and related parties;*
- *Details regarding the enforcement priorities the financial institution believes have been implicated; and*
- *Dates, amounts, and other relevant details of financial transactions involved in the suspicious activity.*
- *"(INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY)" will use the term "MARIJUANA PRIORITY" in the narrative section to help law enforcement distinguish these SARs.*

3. "Marijuana Termination" SAR Filings

If a "GLBS" deems it necessary to terminate a relationship with a marijuana-related business in order to maintain an effective anti-money laundering compliance program, "GLBS" will ask (INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY) to file a SAR and note in the narrative the basis for the termination.

"(INSERT NAME OF PAYROLL PROCESSING BANK/ENTITY)" will use the term "MARIJUANA TERMINATION" in the narrative section.

11. Currency Transaction Reports and Form 8300's

"GLBS" will file CTRs on the receipt or withdrawal by any person of more than $10,000 in cash per day.

Revision History:

- Adopted Sept 2019