APPENDIX 1
BUSINESS PLAN

Southern Country International, Ltd. (SCI) is an International Financial Services Entity (IFSE) in the St. Thomas - St. John District, incorporated in the U.S. Virgin Islands and wholly-owned by Mr. Jeffrey Epstein. SCI's sole office and headquarters are located at American Yacht Harbor, 6100 Red Hook Quarter, St. Thomas, U.S. Virgin Islands. SCI will provide the following lines of business and services while ensuring that, except as specifically indicated below, none of the financial undertakings are granted to domestic persons (i.e., residents of the U.S. Virgin Islands):

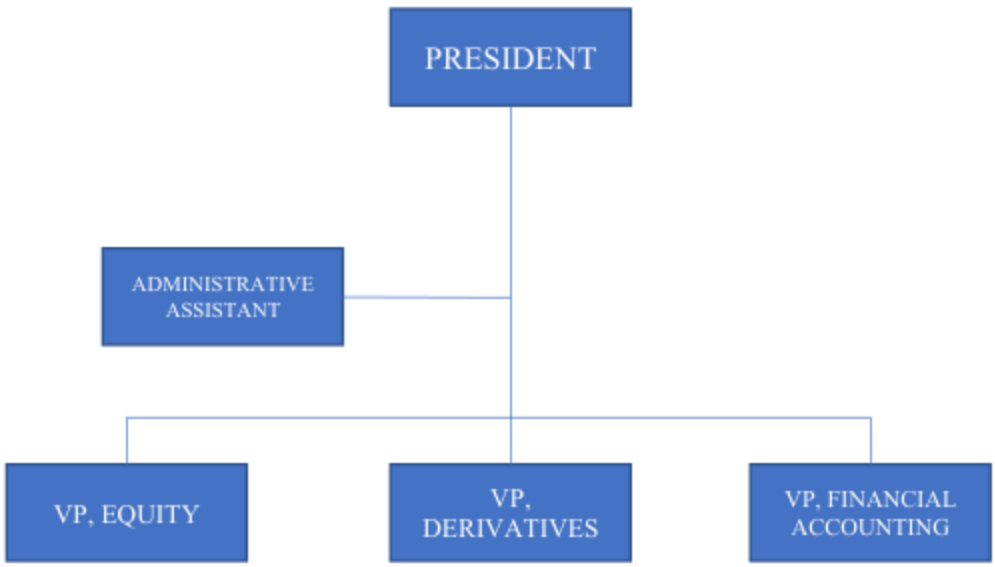
1. SCI may make, arrange, guarantee, secure, bond or service loans or other financial undertakings.
2. SCI may engage in financial and business management services;
3. SCI may make commercial loans in excess of $1,000,000 to U.S. Virgin Islands borrowers that (i) have been rejected, or not approved within 30 days from submission, by any U.S. Virgin Islands financial institution; or (ii) bear interest at an interest rate of not less than five percentage points above the Federal Home Loan Mortgage Corporation's posted yield on the last business day of the month on a thirty-year standard conventional fixed rate mortgage;
4. SCI may make capital contributions in excess of $1,000,000 to U.S. Virgin Islands business entities in the U.S. Virgin Islands;
5. SCI may carry out banking transactions permitted by this chapter in the currency of any country, or in gold or silver, and participate in foreign currency trade;
6. SCI may underwrite, issue, distribute, and otherwise deal in securities, notes, debt, instruments, drafts, and bills of exchange, issued by SCI, or by a foreign person, for final purchase by a person outside of the U.S. Virgin Islands;
7. SCI may buy and sell securities and non-life insurance annuities for clients outside the U.S. Virgin Islands, and provide investment advice in relation to such transactions or separate therefrom, to such persons, and in addition offer these services and products to the Government of the U.S. Virgin Islands and any of its instrumentalities, agencies and investment vehicles;
8. SCI may organize, manage and provide management services to international financial entities, such as investment companies and mutual funds, on the condition that the stock or participation in the capital of such companies is not distributed directly by the IBE to domestic persons; and with prior authorization from the Director, provide to other IBEs or to foreign persons or entities outside of the Virgin Islands, those services of financial nature, as these are defined and generally accepted in the banking industry of the United States and the U.S. Virgin Islands.

SCI may initially focus on the following lines of business:

1. Insurance of non-Virgin Islands risk;
2. Financing of swap transactions and collateralized loan obligations;
3. Other derivative type transactions;
4. Venture capital;
5. Merchant banking; and
6. Wealth management

SCI's initial industry focus on venture capital and merchant banking facilities will target companies in the health and sciences. SCI anticipates providing private equity for start-up and small business sector clients. Private equity will be provided as capital in the form of debt financing, share ownership, and long-term equity with IPO and M & A exit strategies. Private investment companies therefore play a critical role in the global capital markets by providing sources of capital and liquidity to growing business. But beyond capital, they provide operational support, strategic guidance, relationship and networking capabilities, and governance support all aimed at maximizing their investment. They take a long-term perspective on investing and understand that allocating capital requires a rigorous and disciplined approach, and that true value creation comes from providing products or services that possess a unique value proposition in the market. Investment in businesses provides new and better jobs, improved products and services that drive more competition, which in turn improves quality and reduces costs to the end consumer.

APPENDIX 2
ORGANIZATIONAL STRUCTURE



APPENDIX 3
ANTI-MONEY LAUNDERING POLICY & PROCEDURES

This policy has been adopted by SCI in recognition of SCI's obligations under the USA PATRIOT Act, the Bank Secrecy Act, other related money laundering regulations, and the requirements of the United States Virgin Islands Division of Banking, Insurance and Financial Regulation.

SCI will appoint and maintain an anti-money laundering program administrator that is responsible for coordinating and monitoring day-to-day compliance with the all the federal and state laws relating to money laundering. It is the responsibility of the program administrator to coordinate and monitor day-to-day compliance with the detection and prevention of money laundering, including the training of SCI's employees. The management and staff of SCI are committed to implementing policies and procedures that assist us in detecting and preventing money laundering or other illegal activities conducted through transactions with SCI.

THE MONEY LAUNDERING PROCESS

Money laundering is the criminal practice of filtering ill-gotten gains or "dirty" money through a maze or series of transactions, so the funds are "cleaned" to look like proceeds from legal activities. Money laundering does not have to involve cash at every stage of the laundering process. Any transaction conducted with a bank might constitute money laundering. Although money laundering is a diverse and often complex process, it involves three independent steps that can occur simultaneously:

☐ *Placement:* The process of placing, through deposits or other means, unlawful cash proceeds into traditional financial institutions.

☐ *Layering:* The process of separating the proceeds of criminal activity from their origin through the use of layers of complex financial transactions, such as converting cash into traveler's checks, money orders, wire transfers, letters of credit, stocks, bonds, or purchasing valuable assets, such as art or jewelry.

☐ *Integration:* The process of using an apparently legitimate transaction to disguise the illicit proceeds, allowing the laundered funds to be disbursed back to the criminal. Different types of financial transactions, such as sham loans or false import/export invoices, can be used.

POTENTIAL INDICATORS OF MONEY LAUNDERING

A few of the identifiable areas of vulnerability that banks and other depository institutions should be aware of include:

• Structured currency deposits to individual checking accounts, often well below the typical levels for structuring, with multiple daily deposits to multiple accounts at different branches of the same bank on the same day.

• Consumer checking accounts that are used for a period of time and then become dormant. In some cases, the accounts may have become overdrawn, perhaps as a further means of avoiding detection.

• Personal checking accounts opened by foreign nationals who come to the bank together.

• Multiple accounts opened on the same day or held by the same foreign nationals at various banks.
• Increases in the frequency or amounts of currency deposits made by U.S. business accountholders who export to Colombia.

• Suspicious transactions that might be linked to a common scheme. It may also be helpful to develop a dialogue with other financial institution representatives in your area to share ideas and exchange information.

Criminals can also use loan applications for money laundering purposes. This is especially the case when money launderers wish to invest proceeds of crime in real estate. Certain factors should attract the attention of financial institutions, such as:

- A credit application followed by premature repayment of the money withdrawn;
- Repayment of a mortgage loan by means of transfers or deposits in cash disproportionate to the official earnings of the parties involved is also suspicious.
- Transactions linked to tax havens, offshore centers or non-cooperative countries and territories

ANTI-MONEY LAUNDERING DETECTION AND PREVENTION PROCEDURES

Enhanced Due Diligence Account Opening Procedures

Prudent banking practices require that financial institutions know the normal and routine activities of their customers to better serve the customers' banking needs. Additionally, in the U.S. banking environment, the USA PATRIOT Act requires financial institutions to take reasonable steps to ensure knowledge of bank customers' normal and routine business activities. At SCI, these facts present us with many challenges, as many of our customers generally do not have a routine activity. This section of our anti-money laundering policy sets forth SCI's procedures to identify customers when opening accounts, including deposit, loan, and non-deposit accounts such as safe deposit boxes; to identify customers and non-customers wiring money and purchasing monetary instruments; and to identify activities that are suspicious. Through the provisions of this policy, each employee should make an effort to get to know customers that they interact with on a routine or a one-time basis.

Procedures to Open Consumer Accounts

This procedure applies to checking, savings, certificates of deposits, and safe deposit box accounts. The Applicant will obtain and maintain in the customer's file the following information: (If the employee opening the account does not obtain certain information, they must document the reason in the customer file.)

1. Social security number or alien identification number (from U.S. residents);

2. Verification of acceptable identification (e.g., driver's license, state issued photo identification, passport, national identity card for nonresident aliens, etc.);

3. Verification of address of residence;

4. Estimation of anticipated account activity and customer's income source and/or profession;

5. Consideration of the source of funds to open the account;

6. Information obtained from service bureaus to determine whether a customer has been reported for overdrawing accounts, potentially conducting check kiting schemes, etc.;

7. Comparison of the customer with the OFAC and other government lists as directed by our federal regulator and law enforcement;

8. Third-party references; verification services; and telephone, web site, and reverse directories; and

9. Other account relationships.

Procedures to Open Business/Commercial Accounts

SCI will obtain and maintain in a central customer file the following information for all types of business/commercial accounts:
1. Taxpayer identification (ID) number and legal name of business (*if applicable*);

2. Verification of legal status;

3. Verification of identification for principals, their addresses, phone numbers, and if applicable, taxpayer IDs (Please note that SCI's employee personally knowing the customer is not verification of the ID. While that form of verification may satisfy state rules for identity, it does not meet the federal regulators' standards.);

4. Verification of the location of the business. (Please note that this may be documented by a referral from a calling officer or by other means such as a later visit to the business in the first months of the relationship.);

5. Estimate of anticipated account activity;

6. Source of funds to open account;

7. For large businesses, financial statements and a list of the firm's major suppliers and customers;

8. A description of the principal line of business and all types of business operations it engages in;

9. Information from service bureaus to determine the company's previous checking account history;

10. Comparison of the customer with the OFAC and other government lists as directed by our federal regulator and law enforcement;

11. Third-party references; and

12. Other the Applicant's account relationships.

ONGOING REVIEW OF CURRENT CUSTOMERS AND NONCUSTOMERS AGAINST GOVERNMENT LISTS

SCI's policy and procedures for complying with the rules of the Office of Foreign Assets Control (OFAC) is outlined in our separate OFAC policy.

MONITORING FOR SUSPICIOUS ACTIVITY

Management and the anti-money laundering program administrator will ensure that the following reports are monitored for suspicious activity and that employees with the duty to monitor these reports receive adequate internal and external training on detecting money laundering and other illegal activity.

☐ *Suspect kite reports.* These reports identify excessive activity in accounts and should also be reviewed for cash activity. The account profile of an account used for money laundering can be similar to that of an account used for check kiting: high volume of activity, matching deposits and withdrawals, and low average balances in relation to activity.

☐ *Demand deposit activity reports.* These reports cover all customer and employee accounts. They generally show daily balances and accumulate deposits and withdrawals over a thirty (30) day period. These reports may be reviewed manually or management may establish a threshold for certain types of accounts and then review only the exceptions.

☐ *Large transaction reports.* This report will be set at an amount lower than Ten Thousand Dollars ($10,000.00) so that SCI's employees can identify customers who may be structuring transactions to avoid CTR reporting or who have unusual activity in their accounts.

☐ *Incoming and outgoing wire transfer logs.* These logs identify transfers of funds out of the country or to remote banks, transfers funded by cashier's checks or money orders in amounts under the CTR filing threshold, and other suspicious activity of both noncustomers and accountholders.

☐ *Overdraft reports.* This report can be used to assist management to discover whether a previously "good" customer — either individual or commercial — is suddenly having financial problems.

☐ *Commercial service charge analysis reports.* Management is directed to establish thresholds for these reports to monitor a change in your commercial customers' balances, checking, deposit, or currency transactions. Changes in account activity may only mean the company is getting more successful, however management is directed to have these reports reviewed by an objective employee. Although the reviewer may need to discuss the account with the relationship officer, that person should not be the last word on whether the activity in the account is suspicious.

☐ *Delinquent loan reports.* Although these reports generally get special attention, management is directed to pay close attention when delinquent loans are suddenly "cured" with no reasonable explanation in the file. Loan officers must be able to explain a sudden pay-off of seriously delinquent accounts.

☐ *Expired collateral insurance reports.* These reports for personal property and real estate loans are usually the first sign that something is wrong with our loan. Management is directed to instruct operations staff to notify a supervisor or loan officer immediately when a new loan customer fails to purchase initial insurance or renew existing insurance for the collateral, instead of waiting for the notice letters to go out. Whether this is "suspicious" or not depends on what other information we have about this customer.

☐ *Hold notices for Regulation CC.* Management is directed to train operations or customer service staff to notify a supervisor or officer when they hold an unusual check (i.e., in amount or in the location of the drawee bank) on a customer's account for the first time.

SUSPICIOUS ACTIVITY REPORTING

If any of SCI's employee becomes aware of or suspects criminal activity by either SCI's customers or employees, he or she should promptly report the matter to the anti-money laundering program administrator. The anti-money

laundering program administrator will promptly investigate the matter further to determine whether to report the suspicious activity to the Federal Reserve Bank. The investigation will be based on a review of the facts, as submitted by the employee, and a discussion with the supervisors in charge of the affected areas.

Supporting Documentation for the SAR

Except for certain spreadsheets allowed by Financial Crimes Enforcement Network's (FinCEN) e-file system, we will not include supporting documentation with a Suspicious Activity Report (SAR) when it is submitted to FinCEN, but will maintain all documentation that supports the facts and circumstances of the report in the SAR file either in hard-copy, on computer disk or CD, or on relevant software.

Maintaining Accounts After a SAR Has Been Filed

The decision whether or not we will keep an account opened after a SAR has been filed will be made by the President, and may be made on a case-by-case basis. We will document the decision either to close or keep open the account in the SAR file.

If a law enforcement agency requests that we maintain a particular account, we will ask for the request to be submitted in writing from a federal law enforcement agency; it should be issued by a supervisory agent or by an attorney within a United States Attorney's Office or another office of the Department of Justice. If a federal or local law enforcement agency requests that an account be maintained, then we will obtain a written request from a supervisor of the state or local law enforcement agency or from an attorney within our state or local prosecutor's office.

The written request should indicate that the agency has requested that we maintain the account and the purpose of the request. For example, if a state or local law enforcement agency is requesting that we maintain the account for purposes of monitoring, the written request should include a statement to that effect. The request should also indicate the duration for the request. The initial request should not exceed six (6) months. However, law enforcement may make additional requests for the maintenance of the same account after the expiration of the initial request.

Although there is no recordkeeping requirement under the Bank Secrecy Act for this type of correspondence, we will maintain documentation of such requests for at least five (5) years after the request has expired. If we are aware — through a subpoena, 314(a) request, national security letter (NSL), or similar communication — that an account is under investigation, we will notify law enforcement before making any decision regarding the status of the account.

Confidentiality

The anti-money laundering program administrator, and any other staff, including outside counsel aware of SAR related matters, will keep all information related to such matters confidential. SARs are also confidential. Any person subpoenaed or otherwise requested to disclose an SAR or the information contained in an SAR shall decline to produce the information.

If SCI determines it is necessary to report a suspected illegal activity to local law enforcement authorities, the anti-money laundering program administrator will carefully review all known facts. SARs will only be filed when there is a reasonable basis for believing that a specific crime has occurred, is occurring, or may occur. Such reports will be filed with local agencies, other than United States Virgin Islands Division of Banking, Insurance & Financial Regulation subject to the provisions of the Right to Financial Privacy Act.

TRAINING

The anti-money laundering program administrator will conduct or arrange for annual meetings with SCI's personnel who handle currency to keep them informed of any new changes to the Bank Secrecy Act, the USA PATRIOT Act, or other related laws and updates to our anti-money laundering procedures. It is also the responsibility of the anti-money laundering program administrator to train all employees at the time of their initial employment. Additional meetings or other training will be held as necessary to address issues that arise in the interim that must be addressed during the year.

Training may be conducted through presentations at a meeting, circulation of memoranda or other written materials, or any other appropriate manner. A copy of all materials presented or circulated shall be retained by the anti-money laundering program administrator along with a written record of attendance or receipt by the Applicant's personnel.

At least once per year, the anti-money laundering program administrator will attend one (1) external training session relating to the Bank Secrecy Act, fraud detection, or money laundering.

AUDIT PROCEDURES/INDEPENDENT TESTING

At least once each year, an independent audit of the procedures detailed in this policy will be conducted by an external auditor.

Results of the audit will be reported to the President and the anti-money laundering program administrator. It is the responsibility of the anti-money laundering program administrator to take appropriate action to correct any problems found as a result of the audit and respond to the audit committee.