Red Castle Consulting Anti-Money Laundering (AML) Program: Compliance and Procedures

Red Castle Consulting LLC (Red Castle Consulting Group) a domestic LLC business incorporated in the state of Utah (Entity Number: 8536978-0160) in 2013. Red Castle Consulting is a direct investment firm specializing in cryptocurrency, early-stage private investment, and real estate. Red Castle Consulting is not a Broker-Dealer Firm, a Capital Acquisition Broker, or a Funding Portal. As such it is not regulated by the Financial Industry Regulatory Authority (FINRA) (https://www.finra.org/about/firms-we-regulate). As a private investment firm, Red Castle Consulting is not required to have an Anti-Money Laundering (AML) program in place, nor is it subject to Bank Secrecy Act (BSA) filings. Moreover, as a private investment fund the company is not subject to U.S. Securities and Exchange Commission ("SEC") registration as it relies on one of the two exemptions from such registrations found in Sections 3(c)(1) and 3(c)(7) of the U.S. Investment Company Act of 1940 (the "1940 Act" https://www.govinfo.gov/content/pkg/COMPS-1879/pdf/COMPS-1879.pdf).

Despite the lack of legal and regulatory requirements to institute and maintain and AML program, Red Castle Consulting has voluntarily chosen to implement and maintain and AML program patterned after applicable provisions of the BSA and FINRA Rule 3310 (https://www.finra.org/rules-guidance/rulebooks/finra-rules/3310) to ensure that the company's operations and its knowledge of and relationship to its customers complies with the aforementioned laws and regulations:

1. The program is approved in writing by a senior manager.
2. It is designed to ensure the firm detects and reports suspicious activity.
3. It has a risk-based customer identification program (CIP) that enables the firm to form a reasonable belief that it knows the true identity of its customers.
4. It is subject to audit by third parties
5. Ongoing training is provided to appropriate personnel
6. The program must includes appropriate risk-based procedures for conducting ongoing customer due diligence.

I. Firm Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three 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 or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Although cash is rarely deposited into securities accounts, the securities industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of fraudulent activities include insider trading, market manipulation, ponzi schemes, cybercrime and other investment-related fraudulent activity.

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

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable BSA regulations and FINRA rules for a private investment firm and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

II. AML Compliance Person Designation and Duties

The firm has designated Asher Cameron, Vice President Finance & Compliance as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm’s AML program. Mr. Cameron has a working knowledge of the BSA and its implementing regulations and

is qualified by experience, knowledge and training, including key provisions of FINRA Rule 3310. The duties of the AML Compliance Person will include monitoring the firm's compliance with its AML program and overseeing communication and training for employees. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

III. Checking the Office of Foreign Assets Control Listings

Although not part of the BSA and its implementing regulations, the Office of Foreign Assets Control (OFAC) compliance is often performed in conjunction with AML compliance. OFAC is an office of the U.S. Treasury that administers and enforces economic sanctions and embargoes based on U.S. foreign policy and national security goals that target geographic regions and governments (e.g., Cuba, Sudan and Syria), as well as individuals or entities that could be anywhere (e.g., international narcotics traffickers, foreign terrorists and proliferators of weapons of mass destruction). As part of its enforcement efforts, OFAC publishes a list of Specially Designated Nationals and Blocked Persons (SDN list), which includes names of companies and individuals who are connected with the sanctions targets. U.S. persons are prohibited from dealing with SDNs wherever they are located, and all SDN assets must be blocked.

Before opening an account, and on an ongoing basis, Mr. Cameron will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC (http://www.treas.gov/offices/enforcement/ofac/). Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. See also FINRA's OFAC Search Tool that screens names against the SDN list (http://apps.finra.org/RulesRegulation/OFAC/1/Default.aspx). Mr. Cameron will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and he will document the review.

If we determine 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, we 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. We will also call the OFAC Hotline at (800) 540-6322 immediately. Our review will include customer accounts and all transactions involving customers (including activity that passes through the firm such as wires).

IV. Customer Identification Program

We will collect certain minimum customer identification information from each customer and will utilize risk-based measures to verify the identity of each customer; record customer identification information and the verification methods and results; provide the required adequate CIP notice to customers that we will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government.

We do not open or maintain customer accounts within the meaning of 31 CFR 1023.100, in that we do not establish formal relationships with "customers" for the purpose of effecting transactions in securities. If in the future the firm elects to open customer accounts or to establish formal relationships with customers for the purpose of effecting transactions in securities, we will first establish, document and ensure the implementation of appropriate CIP procedures.

i. Required Customer Information

(1) the name;
(2) date of birth (for an individual);
(3) an address, which will be a residential or business street address (for an individual), an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office, or other physical location (for a person other than an individual); and
(4) an identification number, which will be a taxpayer identification number (for U.S. persons), or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

For a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

ii. Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not engage in any business transactions, or will proceed expeditiously to terminate the business relationship. In either case, our AML Compliance Person will be notified so that we can determine what documentation and/or reporting may be required.

iii. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. [Name] will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both. [Tailor the sentence to your actual situation.] We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

• For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and

• For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

• Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source [identify reporting agency, database, etc.];

• Checking references with other financial institutions; or

• Obtaining a financial statement.

We will use non-documentary methods of verification when:
(1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
(2) the firm is unfamiliar with the documents the customer presents for identification verification;
(3) the customer and firm do not have face-to-face contact; and
(4) there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after any business transaction. Depending on the nature of the requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file reports in accordance with applicable laws and regulations.

We recognize that the risk that we may not know the customer's true identity may be heightened for certain types of transactions, such as an account in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified.

iv. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not engage in a transaction; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) terminate transactions after attempts to verify a customer's identity fail; and (4) determine whether it is necessary to file a report in accordance with applicable laws and regulations.

v. Recordkeeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of

any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

NEED:

- Not opening anonymous accounts
- Language that says we don't do correspondent accounts
- Audit and compliance review function to test the adequacy and efficacy of AML policies and procedures
- Policy of protecting employees of they report suspicious activity in good faith

V. Comparison with Government-Provided Lists of Terrorists

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

VI. Customer Due Diligence Rule

We do not open or maintain accounts for legal entity customers within the meaning of 31 CFR 1010.230. If in the future the firm elects to open accounts for legal entity customers, we will first establish, document and ensure the implementation of appropriate CDD procedures.

VII. Correspondent Accounts from Foreign Shell Banks

We will identify foreign bank accounts and any such account that is a correspondent account (any account that is established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank) for foreign shell banks. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Person, who will terminate any verified correspondent account in the United States for a foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by a foreign shell bank but is being used to provide services to such a shell

bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will terminate any correspondent account for which we have not obtained the information described in Appendix A of the regulations regarding shell banks within the time periods specified in those regulations.

We will require our foreign bank account holders to identify the owners of the foreign bank if it is not publicly traded, the name and street address of a person who resides in the United States and is authorized and has agreed to act as agent for acceptance of legal process, and an assurance that the foreign bank is not a shell bank nor is it facilitating activity of a shell bank. In lieu of this information the foreign bank may submit the Certification Regarding Correspondent Accounts For Foreign Banks provided in the BSA regulations. We will re-certify when we believe that the information is no longer accurate or at least once every three years.

We will keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

When we receive a written request from a federal law enforcement officer for information identifying the non-publicly traded owners of any foreign bank for which we maintain a correspondent account in the United States and/or the name and address of a person residing in the United States who is an agent to accept service of legal process for a foreign bank's correspondent account, we will provide that information to the requesting officer not later than seven days after receipt of the request. We will close, within 10 days, any correspondent account for a foreign bank that we learn from FinCEN or the Department of Justice has failed to comply with a summons or subpoena issued by the Secretary of the Treasury or the Attorney General of the United States or has failed to contest such a summons or subpoena. We will scrutinize any correspondent account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these correspondent accounts.

VIII. Due Diligence and Enhanced Due Diligence Requirements for Correspondent Accounts of Foreign Financial Institutions

i. Due Diligence for Correspondent Accounts of Foreign Financial Institutions

We will conduct an inquiry to determine whether a foreign financial institution has a correspondent account established, maintained, administered or managed by the firm.

If we have correspondent accounts for foreign financial institutions, we will assess the money laundering risk posed, based on a consideration of relevant risk factors. We can apply all or a subset of these risk factors depending on the nature of the foreign financial institutions and the relative money laundering risk posed by such institutions.

The relevant risk factors can include:

• the nature of the foreign financial institution's business and the markets it serves;

• the type, purpose and anticipated activity of such correspondent account;

• the nature and duration of the firm's relationship with the foreign financial institution and its affiliates;

• the anti-money laundering and supervisory regime of the jurisdiction that issued the foreign financial institution's charter or license and, to the extent reasonably available, the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered; and

• information known or reasonably available to the covered financial institution about the foreign financial institution's anti-money laundering record.

In addition, our due diligence program will consider additional factors that have not been enumerated above when assessing foreign financial institutions that pose a higher risk of money laundering.

We will apply our risk-based due diligence procedures and controls to each financial foreign institution correspondent account on an ongoing basis. This includes periodically reviewing the activity of each foreign financial institution correspondent sufficient to ensure whether the nature and volume of account activity is generally consistent with the information regarding the purpose and expected account activity and to ensure that the firm can adequately identify suspicious transactions. Ordinarily, we will not conduct this periodic review by scrutinizing every transaction taking place within the account. One procedure we may use instead is to use any account profiles for our correspondent accounts (to the extent we maintain these) that we ordinarily use to anticipate how the account might be used and the expected volume of activity to help establish baselines for detecting unusual activity.

ii. Enhanced Due Diligence

We will assess any correspondent accounts for foreign financial institutions to determine whether they are correspondent accounts that have been established, maintained, administered or managed for any foreign bank that operates under:

(1) an offshore banking license;

(2) a banking license issued by a foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the U.S. representative to the group or organization concurs; or

(3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

If we determine that we have any correspondent accounts for these specified foreign banks, we will perform enhanced due diligence on these correspondent accounts. The enhanced due diligence that we will perform for each correspondent account will include, at a minimum, procedures to take reasonable steps to:

(1) conduct enhanced scrutiny of the correspondent account to guard against money laundering and to identify and report any suspicious transactions. Such scrutiny will not only reflect the risk assessment that is described in Section 8.a. above, but will also include procedures to, as appropriate:

(i) obtain (e.g., using a questionnaire) and consider information related to the foreign bank's AML program to assess the extent to which the foreign bank's correspondent account may expose us to any risk of money laundering;

(ii) monitor transactions to, from or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity (this monitoring may be conducted manually or electronically and may be done on an individual account basis or by product activity); and

(iii) obtain information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account (a correspondent account maintained for a foreign bank through which the foreign bank permits its customer to engage, either directly or through a subaccount, in banking activities) and the sources and beneficial owners of funds or other assets in the payable-through account.

(2) determine whether the foreign bank maintains correspondent accounts for other foreign banks that enable those other foreign banks to gain access to the correspondent account under review and, if so, to take reasonable steps to obtain information to assess and mitigate the money laundering risks associated with such accounts, including, as appropriate, the identity of those other foreign banks; and

(3) if the foreign bank's shares are not publicly traded, determine the identity of each owner and the nature and extent of each owner's ownership interest. We understand that for purposes of determining a private foreign bank's ownership, an "owner" is any person who directly or indirectly owns, controls or has the power to vote 10 percent or more of any class of securities of a foreign bank. We also understand that members of the same family shall be considered to be one person.

iii. Special Procedures When Due Diligence or Enhanced Due Diligence Cannot Be Performed

In the event there are circumstances in which we cannot perform appropriate due diligence with respect to a correspondent account, we will determine, at a minimum, whether to refuse to open the account, suspend transaction activity, file a SAR, close the correspondent account and/or take other appropriate action.

IX. Due Diligence and Enhanced Due Diligence Requirements for Private Banking Accounts/Senior Foreign Political Figures

We do not open or maintain private banking accounts.

X. Monitoring for Suspicious Activity

We will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

XI. Training Programs

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with applicable requirements and implementing regulations under it. This approval is indicated by signatures below.

XII. Senior Manager Approval

Signed: _____

Name:_____

Title: _____

Date: _____