HSAX & Co., LLC
Identity Theft Prevention Program

I. Firm Policy

HSAX & Co., LLC ("HSAX" or the "Firm")'s policy is to protect investors and their accounts from identity theft and to comply with the Securities and Exchange Commission's (the "SEC") Red Flags Rule. We will do this by developing and implementing this written Identity Theft Prevention Program ("ITPP"), which is appropriate to our size and complexity, as well as the nature and scope of our activities. This ITPP addresses 1) identifying relevant identity theft Red Flags for our firm, 2) detecting those Red Flags, 3) responding appropriately to any that are detected to prevent and mitigate identity theft, and 4) updating our ITPP periodically to reflect changes in risks.

Our identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

II. ITPP Approval and Administration

The Firm's Managing Member, Harvey Sax, approved this ITPP. Harvey Sax is the designated identity theft officer and is responsible for the oversight, development, implementation and administration (including staff training and oversight of third party service providers of ITTP services) of this ITPP. Harvey Sax will ensure that this ITPP is provided to and reviewed by all staff of the Firm who have access to nonpublic personal information of investors.

III. Relationship to Other Firm Programs

We have reviewed other policies, procedures and plans required by regulations regarding the protection of our investor information, including our policies and procedures under Regulation S-P and our Privacy Policy in the formulation of this ITPP, and modified either them or this ITPP to minimize inconsistencies and duplicative efforts.

IV. Identifying Relevant Red Flags

To identify relevant identity theft Red Flags, the Firm will monitor the following risk areas:

1. The types of investments offered;
2. The methods used to open the accounts by investors and third parties; and
3. The methods used to access the accounts by investors and third parties.

The Firm will also consider the sources of Red Flags, including identity theft incidents it has experienced and changing identity theft techniques the Firm thinks likely. In addition, we considered Red Flags from the following categories:

1. Suspicious Documents

    a. Documents provided for identification appear to have been altered or forged.

    b. Other information on the identification is not consistent with information provided by the person opening a new covered account or person presenting the identification or information on file with the Firm.

    c. A request for withdrawal of funds appears to have been forged or altered.

2. Suspicious Personal Identifying Information

    a. Personal identifying information provided is inconsistent when compared against external information sources used by the Firm. For example, the Social Security Number ("SSN") has not been issued, or is listed on the Social Security Administration's Death Master File.

    b. Personal identifying information provided by the investor is not consistent with other personal identifying information provided by the investor.

    c. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Firm.

    d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Firm. For example, the address provided for delivery of withdrawal proceeds is fictitious, a mail drop, or a prison.

    e. The SSN provided is the same as that submitted by other clients.

    f. The address provided is the same as or similar to the address submitted by an unusually large number of other prospective clients.

    g. The client fails to provide all required personal identifying information on the withdrawal request form or in response to notification that the withdrawal request form is incomplete.

    h. Personal identifying information provided is not consistent with personal identifying information that is on file with the Firm.

3. Suspicious Account Activity

    a. An account is used in a manner that is not consistent with established patterns of activity on the account. For example, a material change in frequency or amount of withdrawals from an investor's account or a withdrawal request seeks to have the proceeds paid to a different account or address than the one from which the investment was made.

    b. The Firm is notified of unauthorized activity in connection with an investor's account.

4. Notices from Law Enforcement Agencies or Other Sources

Some of these categories and examples may be relevant only when combined or considered with other indicators of identity theft.

V. Detecting Red Flags

The Firm's detection of Red Flags is based on our methods of getting information about investors and prospective investors and verifying it, authenticating persons who access the accounts, and monitoring transactions and change of address requests. Upon opening an account, the Firm will gather identifying information about and verify the identity of the person opening the account through subscription documents. For existing accounts, it can include authenticating investors, monitoring redemptions, and verifying the validity of changes of address.

VI. Preventing and Mitigating Identity Theft

Upon review of the Firm's accounts, how they are opened and accessed, and the Firm's previous experience with identity theft, the Firm has developed our procedures below to respond to detected identity theft Red Flags.

When we have been notified of a Red Flag or our detection procedures show evidence of a Red Flag, we will take the steps outlined below, as appropriate to the type and seriousness of the threat:

Prospective investor. For Red Flags raised by a prospective client:

1. Review the subscription documents. We will review the prospective investor's information collected under the subscription documents (e.g., name, date of birth, address, bank account and an identification number such as a Social Security Number or Taxpayer Identification Number).
2. Seek additional verification. We may also verify the prospective investor's identity by requesting the following information on each type of prospective investor:
    a. Individuals:
        i. Copy of biography page (with photo) of the investor's passport or copy of driver's license;
        ii. Proof of the investor's current address (*e.g.*, current utility bill dated within the last 2 months).
    b. Corporations:
        i. Copy of the memorandum of association or articles of incorporation, or by-laws (or other equivalent documentation);
        ii. Copy of the certificate of incorporation/certificate of trade or the equivalent;
        iii. Certificate of incumbency listing names of beneficial owners and directors of the investor;
        iv. List of duly elected officers of the corporation and their offices, who are duly authorized to execute any and all documents in connection with the investment,

and a copy of the passports or national identity cards and/or document evidencing proof of address (*i.e.*, original utility bill or similar document) of at least two of the authorized signatories.

c. Partnerships:
    i. Copy of the partnership agreement;
    ii. Copy of the certificate of incorporation/formation;
    iii. Copy of the passports or national identity cards and/or document evidencing proof of address (*i.e.*, original utility bill or similar document) of all partners authorized to execute all necessary documents in connection with the partnership's investment.

d. Trusts:
    i. Copy of the trust agreement;
    ii. List of names of all of the trustees containing the current address of such trustees (if not listed in the trust agreement);
    iii. Copy of the passports or national identity cards and/or document evidencing proof of address (*i.e.*, original utility bill or similar document) of all trustees authorized to execute all necessary documents in connection with the Trust's investment;
    iv. A list of the settlors / beneficial owners and the beneficiaries of the trust (if not listed in the trust agreement), together with copies of their passports or national identity cards and/or separate evidence of their address from an official source.

3. Deny the application. If we find that the applicant is using an identity other than his or her own, we will deny the account.
4. Report. If we find that the applicant is using an identity other than his or her own, we will report it to appropriate local and state law enforcement. We may also report it to the Utah Division of Securities.
5. Notification. If we determine personally identifiable information has been accessed, we will prepare any specific notice to investors or other required notice under state law for the state of residency of the affected investors.

Access seekers. For Red Flags raised by someone seeking to access an existing investor's account:

1. Watch. We will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
2. Check with the investor. We will contact the investor to describe what we have found and verify with them that there has been an attempt at identify theft.
3. Heightened risk. We will determine if there is a particular reason that makes it easier for an intruder to seek access, such as an investor's lost wallet, mail theft, a data security incident, or the

investor having given account information to an imposter pretending to represent the firm or to a fraudulent web site.

4. Collect incident information. For a serious threat of unauthorized account access we may collect if available:
    a. Dates and times of activity
    b. Details of any wire transfer activity
    c. Investor accounts affected by the activity, including name and account number, and
    d. Whether the investor will be reimbursed and by whom.
5. Report. If we find unauthorized account access, we will report it to appropriate local and state law enforcement. We may also report it to the Utah Division of Securities.
6. Notification. If we determine personally identifiable information has been accessed, we will prepare any specific notice to investors or other required notice under state law for the state of residency of the affected investors.
7. Review our insurance policy. Since insurance policies may require timely notice or prior consent for any settlement, we will review our insurance policy (as applicable) to ensure that our response to a data breach does not limit or eliminate our insurance coverage.
8. Assist the investor. We will work with investors to minimize the impact of identity theft by taking the following actions, as applicable:
    a. Adding extra security measures before permitting future access to the threatened account;
    b. Offering to change the way the affected investor can make withdrawals from the threatened account; or
    c. Providing the affected investor with information regarding the unauthorized access in order to facilitate investor's ability to seek recourse against the parties that attempted the fraudulent access of investor's account or personal information.

VII. Service Providers

The Firm uses various services providers, such as broker-dealers and custodians, in connection with our clients' accounts. We have a process to confirm that our service providers that perform activities in connection with our clients' accounts comply with reasonable policies and procedures designed to detect, prevent and mitigate identity theft by requiring them to have policies and procedures to detect Red Flags and report them to us or to take appropriate steps on their own to prevent or mitigate identity theft. We will review each service provider's policies and procedures to ensure appropriate identity theft safeguards are in place.

VIII. Updates and Annual Review

The Firm will update this plan whenever we have a material change to our operations, structure, business or location, or when we experience either a material identity theft from a covered account, or a series of related material identity thefts from one or more covered accounts. HSAX will also follow new ways that identities can be compromised and evaluate the risk they pose for our firm. In addition, HSAX will review this ITPP annually to modify it for any changes in our operations, structure, business, or location or substantive changes to our relationship with our clearing firm. Harvey Sax will be responsible to annually update this ITPP as necessary.

IX. Approval

I approve this ITPP as reasonably designed to enable our firm to detect, prevent and mitigate identity theft.

_____
Harvey Sax
Managing Member

Date: _____

HSAX & CO., LLC
Red Flag Identification and Detection Grid

Red Flag	Detecting the Red Flag
Suspicious Documents	
1. Identification presented looks altered or forged.	Our staff who deal with investors and their supervisors will scrutinize identification presented in person to make sure it is not altered or forged.
2. Information on the identification does not match other information our firm has on file for the presenter, like the original account application, signature card or a recent check.	Our staff who deal with investors and their supervisors will ensure that the identification presented and other information we have on file from the account, such as SSN or address are consistent.
3. The request for withdrawal looks like it has been altered, forged or torn up and reassembled.	Our staff who deal with investors and their supervisors will scrutinize each withdrawal request to make sure it is not altered, forged, or torn up and reassembled.
Suspicious Personal Identifying Information	
4. Inconsistencies exist between the information presented and other things we know about the presenter or can find out by checking readily available external sources, such as the SSN has not been issued or is listed on the Social Security Administration's Death Master File.	Our staff will check personal identifying information presented to us to ensure that the SSN given has been issued but is not listed on the SSA's Master Death File.
5. Inconsistencies exist in the information that the investor gives us, such as the withdrawal request asks for the proceeds to be transferred to a different account than the one from which the investment was made.	Our staff will check personal identifying information presented to us to make sure that it is internally consistent.
6. Personal identifying information presented has been used on an account our firm knows was fraudulent.	Our staff will compare the information presented with addresses and social security numbers on accounts or applications we found or were reported were fraudulent.
7. Personal identifying information presented suggests fraud, such as the address provided for delivery of withdrawal proceeds is fictitious, a mail drop, or a prison.	Our staff will validate the information presented when effecting withdrawals by looking up addresses on the Internet to ensure they are real and not for a mail drop or a prison, and will ensure that withdrawal proceeds are requested to the same account from which the investment was originally remitted.
8. The SSN presented was used by someone else opening an account or other investors.	Our staff will compare the SSNs presented to see if they were given by others opening accounts or other investors.
9. The address presented has been used by	Our staff will compare address information to see if

many other people opening accounts or other investors.	they were used by other applicants and investors.
10. A person who omits required information on a withdrawal request form or other form does not provide it when told it is incomplete.	Our staff will track when investors have not responded to requests for required information and will follow up with the investors to determine why they have not responded.
11. Inconsistencies exist between what is presented and what our firm has on file.	Our staff will verify key items from the data presented with information we have on file.
Suspicious Account Activity	
12. An account is used in a manner that is not consistent with established patterns of activity on the account. For example, a material change in frequency or amount of withdrawals from an investor's account or a withdrawal request seeks to have the proceeds paid to a different account than the one from which the investment was made.	We will review account activity as withdrawal amounts become increasingly frequent or high or where a new bank account is used for delivery of withdrawal proceeds.
13. We are notified that there is unauthorized activity in the account.	We will verify if the notification is legitimate and involves a firm account, and then investigate the report.
Notice From Other Sources	
14. We are told that an account has been opened or used fraudulently by an investor, an identity theft victim, or law enforcement.	We will verify that the notification is legitimate and involves a firm account, and then investigate the report.
15. We learn that unauthorized access to the investor's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	We will contact the investor to learn the details of the unauthorized access to determine if other steps are warranted.