Alpha Wealth Funds, LP
Identity Theft Prevention Program & Privacy Program

I. Firm Policy

Alpha Wealth Funds, LP ("ALPHA WEALTH FUNDS" 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. ALPHA WEALTH FUNDS will also follow new ways that identities can be compromised and evaluate the risk they pose for our firm. In addition, ALPHA WEALTH FUNDS 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.

VIIII. Your Privacy Is Important To Us! Our Privacy Policy

This privacy policy has been compiled to better serve those who are concerned with how their 'Personally Identifiable Information' (PII) is being used online. PII, as described in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Please read our privacy policy carefully to get a clear understanding of how we collect, use, protect or otherwise handle your Personally Identifiable Information in accordance with our website.

What personal information do we collect from the people that visit our blog, website or app?
When ordering or registering on our site, as appropriate, you may be asked to enter your name, email address, mailing address, phone number or other details to help you with your experience.
Who is our Data Controller?
All information collected on our site is retained by Day Trade Smart. We do not distribute or otherwise transfer user data to any third party. To contact our Data Controller, please see the bottom of this policy for contact instructions.
When do we collect information?
We collect information from you when you register on our site, fill out a form or enter information on our site.

How do we use your information?
We may use the information we collect from you when you register, make a purchase, sign up for our newsletter, respond to a survey or marketing communication, surf the website, or use certain other site features in the following ways:

- To allow us to better service you in responding to your customer service requests.
- To send periodic emails regarding your order or other products and services.
- To follow up with them after correspondence (live chat, email or phone inquiries)

We do not use user data to make automated decisions regarding user data.
Providing personal information is mandatory to gain access to our software and education. Should personal information not be given, access to our software and education is not possible.

How do we protect your information?
We use regular Malware Scanning.
Your personal information is contained behind secured networks and is only accessible by a limited number of persons who have special access rights to such systems, and are required to keep the information confidential. In addition, all sensitive/credit information you supply is encrypted via Secure Socket Layer (SSL) technology.
We implement a variety of security measures when a user enters, submits, or accesses their information to maintain the safety of your personal information.
All transactions are processed through a gateway provider and are not stored or processed on our servers.

Do we use 'cookies'?

Yes. Cookies are small files that a site or its service provider transfers to your computer's hard drive through your Web browser (if you allow) that enables the site's or service provider's systems to recognize your browser and capture and remember certain information. For instance, we use cookies to help us remember and process the items in your shopping cart. They are also used to help us understand your preferences based on previous or current site activity, which enables us to provide you with improved services. We also use cookies to help us compile aggregate data about site traffic and site interaction so that we can offer better site experiences and tools in the future.
We use cookies to:

- Compile aggregate data about site traffic and site interactions in order to offer better site experiences and tools in the future. We may also use trusted third-party services that track this information on our behalf.

You can choose to have your computer warn you each time a cookie is being sent, or you can choose to turn off all cookies. You do this through your browser settings. Since browser is a little different, look at your browser's Help Menu to learn the correct way to modify your cookies.
If you turn cookies off, Some of the features that make your site experience more efficient may not function properly.It won't affect the user's experience that make your site experience more efficient and may not function properly.

Third-party disclosure
We do not sell, trade, or otherwise transfer to outside parties your Personally Identifiable Information.

Third-party links
We do not include or offer third-party products or services on our website.

Google
Google's advertising requirements can be summed up by Google's Advertising Principles. They are put in place to provide a positive experience for users.
https://support.google.com/adwordspolicy/answer/1316548?hl=en
We use Google AdSense Advertising on our website.
Google, as a third-party vendor, uses cookies to serve ads on our site. Google's use of the DART cookie enables it to serve ads to our users based on previous visits to our site and other sites on the Internet. Users may opt-out of the use of the DART cookie by visiting the Google Ad and Content Network privacy policy.
We have implemented the following:

- Demographics and Interests Reporting

We, along with third-party vendors such as Google use first-party cookies (such as the Google Analytics cookies) and third-party cookies (such as the DoubleClick cookie) or other third-party identifiers together to compile data regarding user interactions with ad impressions and other ad service functions as they relate to our website.
Opting out:
Users can set preferences for how Google advertises to you using the Google Ad Settings page. Alternatively, you can opt out by visiting the Network Advertising Initiative Opt Out page or by using the Google Analytics Opt Out Browser add on.

California Online Privacy Protection Act
CalOPPA is the first state law in the nation to require commercial websites and online services to post a privacy policy. The law's reach stretches well beyond California to require any person or company in the United States (and conceivably the world) that operates websites collecting Personally Identifiable Information from California consumers to post a conspicuous privacy policy on its website stating exactly the information being collected and those individuals or companies with whom it is being shared. – See more at: http://consumercal.org/california-online-privacy-protection-act-caloppa/#sthash.0FdRbT51.dpuf
According to CalOPPA, we agree to the following:
Users can visit our site anonymously.
Once this privacy policy is created, we will add a link to it on our home page or as a minimum, on the first significant page after entering our website.
Our Privacy Policy link includes the word 'Privacy' and can easily be found on the page specified above.
You will be notified of any Privacy Policy changes:

- On our Privacy Policy Page

Can change your personal information:

- By logging in to your account

How does our site handle Do Not Track signals?
We honor Do Not Track signals and Do Not Track, plant cookies, or use advertising when a Do Not Track (DNT) browser mechanism is in place.
Does our site allow third-party behavioral tracking?
It's also important to note that we do not allow third-party behavioral tracking

COPPA (Children Online Privacy Protection Act)
When it comes to the collection of personal information from children under the age of 13 years old, the Children's Online Privacy Protection Act (COPPA) puts parents in control. The Federal Trade Commission, United States' consumer protection agency, enforces the COPPA Rule, which spells out what operators of websites and online services must do to protect children's privacy and safety online.
We do not specifically market to children under the age of 13 years old.
Do we let third-parties, including ad networks or plug-ins collect PII from children under 13?

Fair Information Practices
The Fair Information Practices Principles form the backbone of privacy law in the United States and the concepts they include have played a significant role in the development of data protection laws around the globe. Understanding the Fair Information Practice Principles and how they should be implemented is critical to comply with the various privacy laws that protect personal information.
In order to be in line with Fair Information Practices we will take the following responsive action, should a data breach occur:
We will notify the users via in-site notification

- Within 7 business days

We also agree to the Individual Redress Principle which requires that individuals have the right to legally pursue enforceable rights against data collectors and processors who fail to adhere to the law. This principle requires not only that individuals have enforceable rights against data users, but also that individuals have recourse to courts or government agencies to investigate and/or prosecute non-compliance by data processors.

CAN SPAM Act
The CAN-SPAM Act is a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have emails stopped from being sent to them, and spells out tough penalties for violations.
We collect your email address in order to:

- Send information, respond to inquiries, and/or other requests or questions

To be in accordance with CANSPAM, we agree to the following:

- Not use false or misleading subjects or email addresses.
- Identify the message as an advertisement in some reasonable way.
- Include the physical address of our business or site headquarters.
- Monitor third-party email marketing services for compliance, if one is used.
- Honor opt-out/unsubscribe requests quickly.
- Allow users to unsubscribe by using the link at the bottom of each email.

If at any time you would like to unsubscribe from receiving future emails, you can email us at

- Follow the instructions at the bottom of each email.

and we will promptly remove you from ALL correspondence.

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

_____
Harvey Sax
Managing Member
4-15-19

ALPHA WEALTH FUNDS, LP

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 many other people opening accounts or other investors.	Our staff will compare address information to see if 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.