PRIVACY NOTICE

FAITHWARD ADVISORS
CLIENT PRIVACY

The SEC's Regulation S-P (Privacy of Consumer Financial Information), which was adopted to comply with Section 504 of the Gramm-Leach-Bliley Act, requires the Company to disclose to clients its policies and procedures regarding the use and safekeeping of client records and information. For the purposes of this section and unless otherwise specified, the term "client" refers to the Company's customers, clients, former clients, and prospective clients.

Definitions

Non-public information means personally identifiable financial information and any list, description, or grouping that is derived from personally identifiable financial information.

Personally identifiable financial information is defined to include three categories of information:

1. Information Supplied by client. Any information that is provided by a client or prospective client to the Company in order to obtain a financial product or service. This would include information or material given to the Company when entering into an investment advisory agreement.
2. Information Resulting from Transaction. Any information that results from a transaction with the client or any services performed for the client. This category would include information about account balances, securities positions, or financial products purchased or sold through a broker/dealer.
3. Information Obtained in Providing Products or Services. Any information obtained by the Company from a consumer report or other outside source which is used by the Company to verify information that a client or prospective client has given on an application for advisory services.

Consumer report information means any record about an individual, whether in paper, electronic or other form that is a consumer report or is derived from a consumer report. Consumer report information also means a compilation of such records. Consumer report information does not include information that does not identify individuals, such as aggregate information or blind data.

Information is collected from clients at the inception of their accounts and occasionally thereafter, primarily to determine accounts' investment objectives and financial goals and to assist in providing clients with requested services.

While Faithward strives to keep client information up to date, clients are requested to monitor any information provided to them for errors, and to provide accurate updated information.

Additionally, the SEC has adopted amendments to Rule 30 under Regulation S-P, which require financial institutions to adopt written policies and procedures to properly dispose of sensitive consumer information. The amendments are designed to protect consumers against the risks associated with unauthorized access to information and mitigate the possibility of fraud and related crimes, including identity theft.

REQUIREMENTS

Under Regulation S-P, the Company is required to:

1. Adopt policies and procedures to safeguard client information;
2. Provide an initial Privacy Notice to all clients;
3. Send an updated Privacy Notice if there is a material change in the Company's collection, sharing, or security practices
4. Provide an opt-out notice if the Company shares information with third party non-affiliates.

Regulation S-P requires disclosure of the types of nonpublic personal information the Company collects and whether it shares information with affiliates or non-affiliates. Specifically, the Company's privacy notices must contain the information listed below, unless the disclosure does not apply to the Company's practices at which time the notice can be silent:

1. Categories of nonpublic information collected;
2. Categories of nonpublic personal information disclosed, if applicable;
3. Categories of affiliates and non-affiliated third parties to whom information is disclosed; and

4. Categories of nonpublic personal information disclosed about former clients and the categories to whom the information is disclosed.

DO NOT SHARE POLICY

The Company has a "do not share" policy. The Company does not disclose non-public personal information to non-affiliated third parties, unless an exception exists, as described below. Since the Company currently operates under a "do not share" policy, it does not need to provide the right for its clients to opt out of sharing with non-affiliated third parties, as long as such entities are exempted as described below. If the Company's information sharing practices change in the future, the Company will implement opt out policies and procedures, and make appropriate disclosures to its clients.

Types of Permitted Disclosures - The Exceptions

In certain circumstances, Regulation S-P permits the Company to share non-public personal information about its clients with non-affiliated third parties without providing an opportunity for those individuals to opt out. These circumstances include sharing information with a non-affiliate (1) as necessary to effect, administer, or enforce a transaction that a client requests or authorizes; (2) in connection with processing or servicing a financial product or a service a client authorizes; and (3) in connection with maintaining or servicing a client account with the Company.

The Company's Service Providers

From time to time, the Company may have relationships with non-affiliated third parties (such as attorneys, auditors, accountants, brokers, custodians, and other consultants), who, in the ordinary course of providing their services to us, may require access to information containing non-public information. These third-party service providers are necessary for us to provide our investment advisory services. When the Company is not comfortable that service providers (e.g., attorneys, auditors, and other financial institutions) are already bound by duties of confidentiality, the Company requires assurances from those service providers that they will maintain the confidentiality of non-public information they obtain from or through the Company. In addition, the Company selects and retains service providers that it believes are capable of maintaining appropriate safeguards for non- public information, and the Company will require agreements from its service providers that they will implement and maintain such safeguards.

Processing and Servicing Transactions

The Company may also share information when it is necessary to effect, administer, or enforce a transaction requested or authorized by clients. In this context, "necessary to

effect, administer, or enforce a transaction" includes what is required or is a usual, appropriate, or acceptable method:

1. To carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the client's account in the ordinary course of providing the financial service or financial product;
2. To administer or service benefits or claims relating to the transaction or the product or service of which it is a part;
3. To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the client or the client's agent or broker.

Sharing as Permitted or Required by Law

The Company may disclose information to affiliates and to non-affiliated third parties as required or allowed by law. For example, this may include disclosures in connection with a subpoena or similar legal process, a fraud investigation, recording of deeds of trust and mortgages in public records, or an audit or examination.

Internal Procedures

The Chief Compliance Officer ("CCO") will consider the level of risk that client information may be misused, altered, stolen, or destroyed, and maintain physical, electronic, and procedural safeguards that comply with federal standards to guard each client's personal financial information. The safeguards will:

1. Ensure the security and confidentiality of client records and information;
2. Protect against any anticipated threats or hazards to the security or integrity of client records and information; and
3. Protect against unauthorized access to or use of client records or information that could result in substantial harm or inconvenience to any client.

The CCO will ensure that the following safeguards are maintained:

1. Hard copies of client personal and non-personal financial information including information contained on suitability form will be maintained in the Company's files, and will be secured (locked) after normal business hours;
2. Electronic access to client personal financial information will be restricted to the client's IAR, the CCO and others the CCO determines have 'business need to know' access; and
3. All Associated Persons will be informed of the Company's delivery procedures, security safeguards and destruction/disposal procedures.

DELIVERY PROCEDURES

Initial Privacy Notice Delivery
Each client will be provided with a copy of the Privacy Notice upon opening his/her account. The client is required to acknowledge receipt of the privacy notice in writing, and the acknowledgment will be maintained in the client's file. The privacy notice may be included with Part 2 of Form ADV and acknowledgement of receipt may be included in the written agreement for services/advisory contract.

Revised Privacy Notice
Each client will be promptly provided with a copy of the Company's Privacy Notice if there is a change in the Company's collection, sharing, or security practices.

In all cases, delivery of the privacy notice will be documented in the Company's records and maintained for a period of at least five years.

Disposal of Client Information and Records
Every investment adviser that maintains or otherwise possesses private client information for a business purpose must properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

Disposal means the discarding or abandonment of such information; or the sale, donation, or transfer of any medium, including computer equipment, on which such information is stored.

Based on what is appropriate for the Company's size and the complexity of its operations, the Company has established the following disposal measures:

(i) Records containing client information must be shredded, burned or pulverized so that the information cannot practicably be read or reconstructed;
(ii) Electronic media containing client information must be erased or destroyed in a manner so that the information cannot practicably be read or reconstructed;
(iii) The Company may enter into a contract with a third party engaged in the business of record destruction to dispose of private client information. As part of its due diligence the Company will take reasonable steps to select and retain such service provider that is capable of, and is contractually obligated to, properly dispose of the information.

In this context, due diligence might include reviewing the disposal company's operations, obtaining information about the disposal company from several references or other reliable sources, signing a non disclosure agreement with the disposal company, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.

Managing a Privacy Breach

An Associated Person must immediately notify the CCO if he or she becomes aware of an actual or suspected privacy breach, including any improper disclosure of client non-public personal information and/or of the Company's proprietary information. As appropriate, the CCO will:

- To the extent possible, identify the information that was disclosed and the improper recipients;
- To the extent possible, categorize the incident based on sensitivity of information involved and operational impact;
- Take actions necessary to prevent further improper disclosures;
- Take actions necessary to reduce the potential harm from improper disclosures that have already occurred;
- Discuss the issue with counsel and evaluate individual state reporting requirements;
- Contact regulatory authorities and/or law enforcement officials, where required;
- Notify affected clients, where required;
- Collect, prepare, and retain documentation associated with the breach and the Company's responses, including post-incident review of events and actions taken, if any; and
- Evaluate the Company's existing privacy protection policies and procedures in light of the breach and will make any needed changes accordingly.

Training

Cyber Security training is provided by the KnowBe4 platform and is monitored by the internally by the Operations Manager to ensure completion on an annual basis. The firm will provide guidance and periodic training to employees relating to information security risks and responsibilities. The Company will retain documentation of the agenda of those training sessions and the topics covered. The Company will also retain a dated list of the employees who received such training.

Policy: The SEC's Regulation S-P (Privacy of Consumer Financial Information, hereinafter the "Privacy Rules"), which was adopted to comply with Section 504 of the Gramm-Leach-Bliley Act, requires broker-dealers to disclose to their investors the Firm's policies and procedures regarding the use and safekeeping of investor records ("Privacy Notice").

Among other requirements, the Privacy Rules require financial institutions to send initial Privacy Notices to "consumers" and to provide both customers and consumers the opportunity to opt out of the disclosure of any nonpublic personal information about a consumer to a nonaffiliated third party. The Fixing America's Surface Transportation Act ("FAST") clarifies broker-dealers' obligations with regard to the Privacy Rules. Under the FAST Act, broker-dealers are not required to send annual Privacy Notices to "customers" if the Firm (i) only shares nonpublic personal information with nonaffiliated third parties in a manner that does not require an opt-out right be provided to customers; and (ii) has not changed its policies and procedures with regard to disclosing nonpublic personal information since it last provided a Privacy Notice to customers.

Faithward Advisors has adopted a *Privacy Notice* that it provides to customers when a new account is opened. The Firm may rely on the annual privacy-notice exception when permitted under Regulation S-P, as amended, provided that no material changes have been made to the Firm's sharing practices and disclosures since the most recent notice. The Privacy Notice explains Faithward Advisors' procedures for safeguarding customer information and records and what information, if any, the Firm makes available to outside parties.

The *Privacy Notice* applies to all individual customers of Faithward Advisors, whether US or foreign residents.

<u>"Public" vs. "Nonpublic" Personal Information about Customers</u>

Generally, Faithward Advisors considers information provided to it by a customer or potential customer in the normal course of Faithward Advisors offering a product or service to be "nonpublic personal information." Identifying whether information is "public" or "nonpublic" is important with regard to Faithward Advisors' obligations if Faithward Advisors shares information with nonaffiliated third parties.

For purposes of the amended Regulation S-P, "customer information" includes any record containing

nonpublic personal information about a customer of a financial institution (in any form) that Faithward Advisors maintains or handles, including information about customers of other financial institutions received or maintained by the Firm.

Public information is information that Faithward Advisors reasonably believes may be obtained from three sources:

- Federal state or local government records
- Widely distributed media
- Disclosures to the general public required under federal, state, or local law

"Sensitive customer information" means any component of customer information that, alone or in combination with other information, could create a reasonably likely risk of substantial harm or inconvenience to an individual, including Social Security numbers, driver's license numbers, account access credentials, or biometric identifiers.

Nonpublic personal information also includes any list, description, or other grouping of customers (and publicly available information about them) derived from financial information that is not publicly available.

Sharing Nonpublic Financial Information

In the normal course of business, Faithward Advisors will not share customer nonpublic financial information with service providers such as service bureaus. Agreements with such third parties include assurances regarding the protection of customer records and information. Information sharing with affiliated companies may also occur and this practice, if applicable, is disclosed in Faithward Advisors' *Privacy Notice*.

Faithward Advisors does not share customer nonpublic financial information with non-affiliated companies or non-exempt service providers.

Consistent with the amended Regulation S-P, all contracts with service providers that receive, maintain, process, or otherwise access customer information on behalf of Faithward Advisors must require the service provider to notify Faithward Advisors as soon as possible, but no later than 72

hours, after becoming aware of any incident involving unauthorized access to or use of customer information.

Incident Response Program (New Requirement Under Amended Regulation S-P)

Faithward Advisors maintains a written Incident Response Program reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information. The program includes:

- Assessment of the nature and scope of any incident;
- Identification of customer information systems and data types involved;
- Containment and control measures;
- Eradication and recovery steps; and
- Evaluation of whether sensitive customer information has been, or is reasonably likely to have been, accessed or used without authorization.

If Faithward Advisors determines that unauthorized access to or use of sensitive customer information has occurred, or is reasonably likely to have occurred, Faithward Advisors will provide notice to each affected individual as soon as practicable, but no later than 30 days after discovery of the incident, unless delayed for legitimate law-enforcement needs.

The notice will include the elements required under Regulation S-P, including a description of the incident, the type of information involved, and guidance on steps customers may take to protect themselves.

Protection of Customer Information And Records

Faithward Advisor's protection of customer information and records includes the following procedures:

- Faithward Advisors provides customers with a copy of its Privacy Notice when new accounts are opened.
- Accounts that opt out will be coded to prevent the release of nonpublic financial information to nonaffiliated third parties.

- Electronically stored customer information is protected by passwords or other established controls within the Firm's system to ensure only authorized persons gain access.
- Faithward Advisors protects its website with firewalls, a secure server, and anti-virus programs.
- Meraki firewall secures the company network separate from guests.
- SentinelOne Anti-virus is installed on every computer/endpoint
- 24/7 monitoring of endpoints and email for any possible security breaches through MDR.
- Requests for customer information from outside parties such as regulators, the Internal Revenue Service, and other government or civil agencies are referred to Compliance for review and response.
- All agreements with other service providers include the third party's privacy policy and must comply with the service-provider oversight requirements described above.
- Faithward Advisors will follow the incident response and customer-notification requirements under amended Regulation S-P.

Disposal of Consumer Report Information and Records

Consumer report information and records must be disposed of in a manner that prevents unauthorized access or use. To accomplish this, Faithward Advisors takes the following steps:

- It designates and trains specific associated persons to dispose of such information properly.
- It ensures that electronic information is destroyed or erased such that it cannot be practicably read or reconstructed.
- It ensures that paper documents containing such information are burned, pulverized, or shredded so that they cannot be practicably read or reconstructed.
- It ensures that trash containing destroyed media or documents involving consumer report information is securely removed.

In accordance with the amended Regulation S-P, Faithward Advisors will maintain written records of:

- The Firm's policies and procedures under the Safeguards Rule and Disposal Rule;
- Its Incident Response Program;
- All investigations of security incidents and determinations related to sensitive customer information;
- All customer notifications made as a result of incidents; and
- Service-provider oversight activities and related communications.

Supervision: The CCO, or designee, shall retain a copy of the Privacy Notice sent, and shall make and retain a record of its distribution. The CCO shall also oversee compliance with the Firm's Incident Response Program and service-provider oversight obligations.

SEC Regulation S-AM

Policy: SEC Regulation S-AM ("Limits on Affiliate Marketing") limits use of certain information received from an affiliate to solicit a consumer for marketing purposes unless the consumer has been given notice and a reasonable opportunity and a reasonable and simple method to opt out of such solicitations. Regulation S-AM applies to all individual customers of the Firm, whether US residents or foreign residents.

Regulation S-AM policies regarding the safeguarding of customer information and records, and whether the Firm shares information with outside parties, are included in the Firm's Privacy Notice.

Procedures: The Firm provides all new customers with a copy of its Privacy Notice upon account creation and on an annual basis thereafter.

As part of this procedure, the Firm also must provide an Opt Out notice to all customers, which is included in the Privacy Notice. Accounts that opt out will be coded to identify clients whose information should not be shared with affiliates for their marketing purposes.

Supervision: The appropriate Designated Principal will ensure that customers receive a copy of the Privacy Notice containing the Regulation S-AM opt-out provision on account inception and annually thereafter.

In addition, the Designated Principal will ensure that agreements with third parties receiving customer information reflect the third-party firm's privacy policies. This responsibility is part of the overall supervision duties related to third-party arrangements.

Identity Theft Program (Fair and Accurate Credit Transactions Act of 2003, Section 114 and 315; SEC Regulation S-ID)

Policy: The FTC and the federal banking regulators have issued joint regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"). The FTC's

Red Flags Rule requires a member firm that is a “financial institution” or “creditor” offering or maintaining “covered accounts” to develop, implement, and administer a written Identity Theft Prevention Program (“ITP Program”) to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or the maintenance of any existing covered account. The Red Flags Rule also requires every member firm that is a financial institution or creditor to periodically reassess whether it offers or maintains covered accounts that would require it to have in place a written ITP Program.

On April 10, 2013, the SEC and the Commodity Futures Trading Commission ("CFTC") jointly adopted the Regulation S-ID: Identity Theft Red Flags Rules ("Red Flags Rules") and guidelines as mandated under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. The Red Flags Rules require broker-dealers and CFTC-regulated entities to implement programs to prevent, detect, and mitigate the effects of identity theft if that entity directly or indirectly holds a "transaction account" belonging to a customer. The Red Flags Rules require each "financial institution" and "creditor" that offers or maintains one or more "covered accounts" (defined below) to develop and implement a written Identity Theft Prevention Program. "Financial institution" is defined as any entity such as certain banks and credit unions and any other person that directly or indirectly holds a transaction account.

Definition of “Financial Institution” and “Creditor”

The term “financial institution” is defined to include any “person that, directly or indirectly, holds a transaction account belonging to a consumer.” A “transaction account” includes any account that allows the account holder to make withdrawals by negotiable or transferable instrument, payment orders, telephonic transfers or similar transactions for the purpose of making payments or transfers to third persons. A “consumer” is defined to include natural persons.

Examples of arrangements that could cause the broker-dealer to be deemed a financial institution for purposes of the Red Flags Rules include a broker-dealer with the ability to direct transfers or payments from one or more natural persons’ accounts to third parties, either unilaterally or upon the instructions of the natural person account owners.

Periodic Assessments

The Red Flags Rules require each broker-dealer that is a financial institution to periodically assess whether it offers or maintains any covered accounts. "Covered accounts" are defined to include:

- An account that is primarily for personal, family or household purposes that is designed to permit multiple payments or transactions; and
- Any other account for which there is a reasonably foreseeable risk from identity theft to natural person customers or to the safety and soundness of the Firm.

The assessment as to whether a broker dealer maintains any covered accounts must include evaluations of:

- The Firm's method for opening accounts;
- The ways in which clients and investors can access accounts; and
- The Firm's prior experiences with identity theft.

A business supervisor, including but not limited to the CEO or others, in consultation with Compliance, will carefully analyze its customers and accounts to determine the extent to which it must comply with the FTC's Red Flags Rule and SEC Regulation S-ID.

The Firm does hold covered accounts[1] for individuals; and therefore would be considered a "financial institution" and is subject to the Red Flags Rule and SEC Regulation S-ID.

Policy: The Firm may receive instructions from a customer to withdraw or transfer funds or securities by email.

Procedures and Supervision: In such instances, the Designated Principal will confirm that the email has been authorized by the customer if it is pursuant to a previously written authorization to use that specific email address (e.g. on the new account form or in a written instruction). This email

[1] A covered account is defined in SEC Regulation S-ID as (i) an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

instruction will either be confirmed by the Designated Principal or designee at the time of the request, or the notification of the request will be sent to the customer. A notation of this confirmation/notification will be recorded. If the request involves the forwarding of funds or securities to a third party or unknown party, the Designated Principal will consult with the CCO if the customer cannot be contacted to confirm the request. This will be especially considered if the request is overly urgent or otherwise inconsistent with the experience with that customer. The Designated Principal will consider whether such a request should be delayed until the customer can confirm the instructions.

Customers will also be advised that they should contact the Firm if their email has been compromised. This will be done either through a notice sent by the clearing firm, in annual disclosure documents, or on the Firm's website.

Confidential Information

Policy: Faithward Advisors may at times have confidential information. Much of that information comes from clients. On other occasions, Faithward Advisors creates confidential information for its clients or for its own use. The proper use and handling of confidential information may vary depending upon the nature of the information, the source of the information, and the context in which the information was obtained or created.

The confidential information procedures apply to all Faithward Advisors associated persons, regardless of specific job responsibilities, department, or location. Every associated person has an obligation to become familiar with and to comply with these policies and procedures, as well as any supplemental policies and procedures applicable to that associated person (e.g., regional or business group policies).

Strict adherence to confidential information policy is critical in maintaining the reputation of the Firm's integrity and trust of clients and counterparties. Failure to comply may create an appearance of impropriety that causes damage to Faithward Advisor's reputation. It may also subject Faithward Advisors to legal and financial liability as well as regulatory sanctions.

<u>Temporary Associated Persons, Contractors and Consultants</u>

Temporary associated persons, contractors and consultants are bound by confidentiality agreements as specified in their contracts. In most instances, however, it is appropriate to require

the temporary associated person, contractor or consultant to comply with the policies and procedures described herein. Temporary associated persons, contractors and consultants will be required to attest to these procedures and other applicable policies and procedures in Comply.

Former Associated persons

An individual who ceases to be an associated person of Faithward Advisors has a continuing obligation to maintain the confidentiality of inside and proprietary information as long as the individual possesses inside or proprietary information learned during the course of the individual's employment or affiliation with Faithward Advisors.

"Need to Know" and "Least Privilege" Policy

The Firm has a "need to know" policy grounded upon the idea of "least privilege" with respect to the disclosure of confidential information. Associated persons are expected to limit disclosure of the access to confidential information only to those persons who. Privilege extends to shared files on the server that are managed via security groups. This is based on approved requests for associates who:

- Must have the information to serve the proper business purposes of the Firm; or
- Must have the information to serve the proper business purposes of the clients; and
- Can be expected to maintain the information in confidence.

Examples: The Firm's outside counsel, the client's accountants or attorneys may be in "need to know" position.

The people that may "need to know" should be those that are:

- Personnel and external advisers directly involved in the transaction,
- Managers of people that are involved in the transaction, and
- Fulfilling corporate control functions.

Associated persons may not disclose:

- Confidential information to any person under any circumstances in which it appears likely that such person will misuse the information;
- Inside information; and
- Clients' personal information to third parties, except as permitted by the Firm's privacy policies.

Protecting Confidential Information

Associated persons should not discuss confidential information in public places such as hallways, elevators, taxis, airplanes, airports, subways, trains, and restaurants. Speaker phones should not be used in circumstances where confidential information may be overheard. Mobile phones, emails and other means of electronic communications may not be secure. Associated persons should use them with care. Associated persons may only use firm-authorized email and instant messaging systems when discussing confidential information.

Access to Office Areas and Physical Separation of Business Units

To the extent possible, access to office areas where confidential information may be observed or discussed should be limited to persons with a business reason for being in the area. Firm policy requires that areas where confidential information is accessible or stored are appropriately segregated and secure.

To the extent appropriate, Faithward Advisors will physically separate business units that are engaged in its advisory and investment management activity from business units.

Associated persons must act in a manner that is consistent with these physical barriers to the flow of confidential information.

Access to Documents and Technology

Documents should not be placed in office areas where unauthorized persons may have access to them. Confidential documents should be stored in locked file cabinets or other secure locations when they are not in use, and they should not be left exposed on desks, printers, fax machines, copiers, or in work rooms or other locations that are not secure.

Code names or numbers should be used for projects that may involve material non-public information. Where code names or numbers have been assigned to a project, internal documents and emails generated with respect to the project should use only the relevant code names and numbers.

Databases and other sources that contain confidential information and are accessible by computer or other technological means should be password-protected or otherwise secure from access by unauthorized persons. Access rights should be reviewed on a periodic basis to ensure that persons accessing systems remain authorized.

Our data protection protocols include:

- Access Controls: All databases and systems storing confidential information are password-protected and restricted to authorized personnel only.
- Password & Session Security: We enforce a strong password policy and automatic screen lockout measures following periods of user inactivity.
- Regular Access Audits: System access rights are reviewed periodically to ensure that only individuals with a legitimate business need maintain active access permissions.
- Routine Security Reviews: We conduct regular, ongoing assessments—including annual reviews of server files and security groups—to evaluate and strengthen our data security position.

<u>Confidentiality Obligation Continues after Termination of Employment</u>

If employment at Faithward Advisors is terminated for whatever reason, the former Faithward Advisors associated person is required to keep confidential all Faithward Advisors proprietary information and non-public information concerning Faithward Advisors clients or prospective clients. The associated person is not permitted to take any such information away after employment is terminated.

Procedures: Unless otherwise specified, information about client orders, portfolios and investment intentions are to be treated as confidential and should not be disclosed except as necessary to serve the business purposes of the client. Confidential information may be used only for the specific purposes for which the client, prospective client, or other third-party provided it to Faithward

Advisors. Any other use of confidential information is a misuse unless the permission is granted by the source that originally provided the information to Faithward Advisors.

Proprietary information may be used only in a manner that is consistent with the specific purposes for which it was created or obtained by Faithward Advisors. Any other use of proprietary information is a misuse unless specific approval is received from Compliance.

Information about Faithward advisor's proprietary activities (including its advisory, banking, and investing activities) and relationships (such as relationships with service providers, consultants and vendors) may also be confidential proprietary information that should not be disclosed except as necessary to serve the business purposes of the Firm and, where necessary, appropriate permissions have been obtained.

Failure to comply with the confidential information procedures may be grounds for disciplinary action, including termination of employment. In addition, failure to comply with these policies and procedures may subject an associated person to civil and criminal penalties, which may include imprisonment, fines, and the suspension or loss of the violator's license or approval to engage in the securities business.

All questions regarding the scope and application of the use of confidential information should be directed to Compliance. If an associated person is uncertain of whether information they possess is confidential information, they should consult with Compliance prior to using or disclosing information in question.

Certification

Every associated person and any other person subject to associated person policies is required to certify to Faithward Advisors that they have read and understood the confidential information procedures and are complying with those policies and procedures.

Confidential Information and Trading Restrictions

An associated person may not purchase or sell a security, cause the purchase or sale of a security, or recommend or solicit the purchase or sale of a security for any account while in possession of confidential information relating to that security.

The prohibition on trading does not apply to certain transactions that are executed in accordance with a pre-existing plan or instruction that complies with certain legal requirements.

In addition, trading restrictions in associated person accounts may be restricted by any watch, restricted list, or special list where a potential conflict of interest might arise.

Supervision: Designated Principals are responsible for their respective business and support groups adhering to confidential information policies and procedures.

Compliance has overall responsibility for advising business management regarding policies and procedures for handling confidential information.

Procedures for Reporting Actual or Potential Unauthorized Breach

Any associated person who has reason to believe that they or someone else has obtained or disclosed confidential information in a manner not permitted by the Firm policies should contact Compliance. In such circumstances, the associated person must not use or further disclose the information.

Safeguarding Customer Records and Information in Network Storage

5/23/19 OCIE Risk Alert – Safeguarding Customer Records and Information in Network Storage - Use of Third Party Security Features

Policy: Faithward Advisors has developed procedures designed to address "Safeguarding Customer Records and Information in Network Storage." These procedures also address the use of security devices offered by third-party storage providers. In addition, the procedures are designed to combat unauthorized access to information stored on the device, and weak or misconfigured security settings on a network storage device. The SEC has observed that firms do not always use the available security features.

The Office of Compliance Inspections and Examinations ("OCIE") identified security risks associated with the storage of electronic customer records and information by broker-dealers and investment advisers in various network storage solutions, including those leveraging cloud-based

storage. The level of threat and susceptibility is unpredictable in a constantly changing environment.

The Information Technology Department ("IT") will be responsible for ensuring implementation of a configuration management program that includes data classification, vendor oversight, and security features that would mitigate the risks incurred when implementing on-premise or cloud-based network storage solutions. Effective configuration management programs, data classification procedures, and vendor management programs include features such as the following:

- Specifications to support the initial installation, ongoing maintenance, and regular review of the network storage solution
- Guidelines for security controls and baseline security configuration standards to ensure that each network solution is configured properly
- Vendor management policies and procedures that include, among other things, regular implementation of software patches and hardware updates followed by reviews to ensure that those patches and updates did not unintentionally change, weaken, or otherwise modify the security configuration.
- Patch Management: Windows operating systems and common third-party software are centrally managed through our Remote Monitoring and Management (RMM) platform. Standard software patches are subject to a seven day delay/approval period prior to deployment to ensure system stability.

On a periodic basis, IT will verify that security settings on network storage solutions designed to protect against unauthorized access are configured adequately. Additionally, IT will review security settings on vendor-provided network storage solutions to confirm that their configuration meets the Firm's standards.

Responding to Privacy Incidents and Breaches

Consistent with the Faithward Advisors Privacy Policy and Faithward Advisors Incident Response Plan, if any employee becomes aware of an actual or suspected privacy incident or breach, including any improper disclosure of nonpublic personal information, that employee must promptly notify the CCO and CEO. Upon becoming aware of an actual or suspected incident or breach, IT, in consultation with the CCO and/or CEO, will investigate the situation and take the following actions as appropriate:

- To the extent possible, identify the information disclosed and the improper recipients.

- Notify appropriate members of senior management.
- Take any actions necessary to prevent further improper disclosures and document all compensating controls.
- Take any actions necessary to reduce the potential harm from improper disclosures that have occurred.
- Discuss the issue with legal counsel and consider discussing the issue with regulatory authorities and/or law enforcement officials.
- Assess notification requirements imposed by applicable state and national regulatory authorities and/or law enforcement officials.
- Evaluate the need to notify affected investors and make any such notifications.
- Collect, prepare, and retain documentation associated with the inadvertent disclosure and Faithward Advisor's response.
- Evaluate the need to change Faithward Advisor's privacy protection policies and procedures in light of the incident or breach.