INFORMATION PROTECTION
AND
IDENTITY THEFT PREVENTION PROGRAM

BATES SECURITIES, INC.

These procedures were approved by George E. Bates, CCO. These procedures are effective from the date approved until the date of their authorized revision, update or replacement (see below).

Authorized Approval Signature: George E Bates

Date these procedures became effective: 12/28/2020

Date these procedures were no longer effective (date of revision, update or replacement): _____

Recordkeeping: Discard after _____ (date three years from termination of use).

TABLE OF CONTENTS

INTRODUCTION

Over the past decade, the incidence of breaches of confidential information and identity theft has grown exponentially. To address these problems, the federal government and most states have adopted rules and regulations to try to protect non-public information and protect the identity of individuals. While most states only require notification once a breach has been detected, the Commonwealth of Massachusetts has enacted a law that requires firms that do business with Massachusetts residents, and that receive or store non-public information on these residents, to develop procedures to protect this information at all times, to educate their personnel regarding these requirements, and to inform the state of any breaches to their information systems.

Bates Securities, Inc. is committed to protecting the non-public information it possesses on its customers, employees and vendors to help mitigate the risk of identity theft without regard to their state of residence.

Bates Securities, Inc. does business with individual investors and gathers non-public information about these investors for the purpose of securities transactions on behalf of these individuals. In addition, the Company gathers non-public information about its employees, registered representatives and other associated persons, as well as vendors with whom it has contracts. Therefore, the Company is subject to certain requirements under Reg. S-ID, Regulation S-P and most state identity protection rules.

PART I: REGULATION S-ID

Reg. S-ID requires financial institutions and creditors, as defined by the Act, to establish procedures to identify "red flags" during various stages of the relationship with their customers and to take action to mitigate damages that could occur from breaches in their information systems. Reg. S-ID provides the following relevant definitions:

- "Financial institution" means a depository or other institution that directly or indirectly holds a transaction account belonging to a consumer.
- "Transaction account" means an account that permits the account holder to make withdrawals for payment or transfer to third parties of securities or funds via telephone transfers, check, debit card or similar items.
- "Consumer" within these definitions refers only to individuals as customers, not institutions.
- "Creditor" means any person who regularly extends, renews, or continues credit or regularly arranges for the extension, renewal or continuation of credit. This would include introducing or clearing firms providing margin, or firms arranging loans, even if for institutional customers.
- "Covered accounts" means (1) an account offered or maintained primarily for personal, family or household purposes that is designed to permit multiple payments or transactions—e.g., "retail" accounts; or (2) any other accounts, including institutional accounts, if they pose a foreseeable risk to the Company's customers or to its own safety and soundness from identity theft.

Given these definitions and the Company's business:

The CCO has determined that the Company meets the definition of a "financial institution" (or a "creditor") and as such is required to implement a Written Identity Theft Program that identifies potential "red flags" and steps to address such actions. The Company's Red Flag Procedures are described below.

Credit or Debit Cards: Reg. S-ID also provides for specific procedures to be followed where an entity issues credit or debit cards. The Company does not issue credit or debit cards. It is therefore not required to have procedures in place to assess the validity of any address change notifications it receives.

Consumer Reports: A component of Reg. S-ID that may apply to some broker-dealers relates to the use of consumer reports. In reviewing the Company's business, the designated Principal has determined that the Company does not request consumer reports on individuals from consumer reporting agencies (CRAs) and, therefore, is not required to have procedures addressing the receipt of notices of address discrepancy from CRAs.

Red Flag Procedures

Identifying misuse or misappropriation of customer information can be difficult and can occur during various stages of the Company's relationship with a customer. To assist in identifying possible incidents of misuse of customer information or identity theft, registered representatives and other Company personnel must be vigilant in reviewing and monitoring account documentation and customer requests.

A way in which representatives can help identify potential identity theft is through information gathered during the account opening stage and throughout the customer relationship. The Company has procedures in place related to knowing customers and verification of identity that can be found in the Company's Written Supervisory Procedures and Anti-Money Laundering Program. Registered representatives and associated personnel should pay particular attention to the following when opening new accounts or when gathering information from a new customer:

Suspicious documents:

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the ID is inconsistent with the appearance of the person presenting the ID.
- Information on the ID, such as the date of birth or address, is inconsistent with information provided on the new account form or other documents presented to open an account.
- Information on the new account form is inconsistent with information already received from the customer or on application documents.
- An application appears to have been altered or forged or appears to have been destroyed and reassembled.

Suspicious personal identifying information:

- Information that is inconsistent with external information sources used by the financial institution or creditor, such as:
    - the address does not match any address in the consumer report; or
    - the Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- Information provided is not consistent with personal identifying information provided on other documentation, such as investment applications.
- Information provided is of a type commonly associated with fraudulent activity, as indicated by internal or third-party sources, such as:
    - the address on an application is fictitious, a mail drop, or a prison; or
    - the phone number is invalid, or is associated with a pager or answering service.
- The SSN, address or telephone number is the same as that submitted by other persons opening an account or other customers.
- The person opening the accounts fails to provide required personal identifying information or does not respond to requests for the information.
- Information is not consistent with other information on file that is related to the customer name provided.

Once an account has been established, registered representatives and other Company personnel should remain vigilant to detect possible incidences of identity theft or account breaches. Indicators of potential problems with established accounts can include:

- Changes in the address of record to fictitious locations, mail drops and PO Boxes without a physical residence also being included on the account, or addresses outside the geographic area where the account holder is known to reside.
- Mail returned as undeliverable.
- Activity in the account that is inconsistent with the customer's investment objectives or normal trading patterns.
- Liquidation of the entire account or significant portions thereof, accompanied or followed by a request to send a check or wire transfer to a third party or to an address or bank that is not recorded in the account record.

- Signatures on letters of authorization, changes of address or other requests that are not consistent with signatures on other documents obtained for the account.
- Requests to journal or transfer cash or account holdings to accounts of third parties.
- Reluctance or refusal to provide more information or documentation when requested.
- Inability to provide information about the account or account owner, if requested, during telephone conversations about the account.

Registered representatives or other Company personnel that suspect possible identity theft or misappropriation of account information should review their suspicions with their supervisor, compliance or another designated Principal so the Company can determine the validity of the suspicions and take actions to try to determine what steps to take to protect the customer.

Principals in their review of transactions will also watch for potential indications of identity theft or misappropriation of account information.

The CCO will also monitor notices and warnings received from other financial institutions, law enforcement or other third parties relating to potential identity theft or other illegal activities. The designated Principal will review a list of the Company's customers, as well as documentation related to potential new customers, to determine if such notices are related to any individuals doing business with, or seeking to do business with, the Company. If he or she determines that such an individual has an account with the Company or is attempting to engage in business with the Company, he or she will investigate the circumstances and will notify the appropriate regulatory or law enforcement agency promptly.

Procedures to Mitigate Risk

The Company conducts mutual fund, variable insurance product, variable annuity or 529 plan business via check and application. The Company does not hold customer accounts, funds or securities directly and relies on the product issuer/sponsors to have systems and procedures in place to protect accounts from unauthorized access or misappropriation of customer information. Reliance on the product issuers/sponsors does not diminish the Company's responsibility to be vigilante in trying to identify potential "red flags" or for bringing suspected breaches to the attention of the clearing firm, customer and appropriate regulatory or law enforcement agencies as warranted.

The Company also implements the following procedures to help protect access to accounts or other information:

- Multifactor Authentication along with username and password is used to access company computers, client relationship management system, portfolio management software, custodial platforms, and company email.
- Passwords will be set up to include a combination of numbers, letters and special characters.
- Access to systems will be locked if someone attempts to login more than 3 times with an incorrect login id/password combination. Only the CCO or Backoffice Administrator can reset a password that has been locked.

Customers are encouraged to also be vigilant in reviewing their account information and to notify the Company and/or the product issuer/sponsor of any discrepancies as soon as possible.

Registered representatives and other Company personnel who have access to customer account information will be required to review the Company's procedures upon hire and will receive

training at least annually on any changes to rules, regulations or procedures related to Reg. S-ID. The CCO will maintain a record of training in each person's registration or personnel file.

Personnel who have reason to believe that a customer has been the victim of identity theft or that an account has been compromised must immediately bring this information to the attention of the CCO. Failure to do so will result in prompt and documented disciplinary action and may result in criminal or civil penalties if the identity theft or misappropriation is proven.

PART II – PROTECTION OF NON-PUBLIC INFORMATION

Non-public personal information is generally defined as information received from a natural person that includes the person's first and last name or first initial and last name, plus one or more of the following:

- The person's complete social security number;
- A complete financial account or credit/debit card number; or
- A complete government-issued identification number, including but not limited to a driver's license number or passport number.

The Company gathers non-public information, as defined above, on the following individuals during the normal course of business:

- Customers or potential customers/investors,
- Employees or registered representatives, and
- Vendors or independent contractors engaged by the Company.

The Company shall only gather that information necessary to conduct its business and provide products and services to its customers and employees. Only personnel required to have such information in order to fulfill the purpose for which it is gathered shall have access to the information. The persons designated to review certain areas of the organization, such as the CCO, shall review the information gathered by their respective areas of supervision to determine that only information required to fulfill that areas responsibilities is being gathered and that persons not authorized to receive the information do not have access to such.

The Company has evaluated the types of non-public personal information received and the potential risks regarding the security, confidentiality and integrity of such information. To comply with various state and federal requirements related to the protection of non-public personal information, the Company has developed procedures to protect the information at various stages of use within the Company, to provide training to its personnel relating to the protection of such information and to detect and prevent breaches.

All persons who may have access to non-public information will be trained on Company policies and regulatory requirements when hired. In addition, the Company shall provide annual training to any persons with access to such information, persons responsible for the implementation of Company policies, and IT personnel or vendors as deemed necessary based on changes to policies, rules or regulations and the type of information being gathered or retained. The Company will keep records related to training in the individual's personnel or vendor file.

Registered representatives, operations personnel and all other persons in the Company with access to non-public personal information gathered by the Company must be familiar with these procedures and must adhere to them at all times. Failure to follow Company procedures as outlined throughout this Manual or to report potential breaches to the security of non-public personal information shall result in disciplinary action. The types of disciplinary action to be taken will be determined by the applicable Principal or manager based on the facts and circumstances of the situation as well as its severity.

SECTION 1: INFORMATION GATHERING

Information is gathered from various individuals prior to or at the time they become associated with the Company. This information can be gathered in various ways and is used for different purposes, depending on the relationship with the Company. In all cases, non-public information must be gathered in such a manner as to prevent unauthorized access to the information. Non-public information must be maintained in a private location and in a manner determined by the Company, such as new account forms or employment applications. Information should not be recorded on documents or in a manner not consistent with Company policies and when Company personnel take information over the telephone, the information should not be repeated in areas where persons not entitled to the information may overhear the conversation.

SECTION 2: TRANSMISSION AND DELIVERY OF INFORMATION

Company personnel are responsible for the security of non-public information from the time it is received until it is eventually disposed of by the Company at the end of the relationship with the customer, employee or vendor. The process of delivering information to the Company's files following its receipt is important as failure to deliver information properly can result in the information being compromised or stolen. The CCO is responsible for ensuring that the Company's policies related to the delivery of non-public information are followed and that any misappropriation or loss of such information is immediately reported to:

- The individuals whose information was compromised, and
- Applicable state or federal regulatory or law enforcement agencies.

2.1 Paper Document or Fax Delivery

When information is captured on paper and must be delivered to the Company from an external location, it is very important that the delivery of this information is secure. Failure to keep control of documents during physical delivery or failure to verify fax numbers can result in information being obtained by unauthorized persons or being lost.

Personnel charged with delivering information to the Company's files from external locations must keep it in secure, locked vessels when available or must ensure that information is kept from the sight of others and it is kept in their control at all times.

When faxing non-public information, Company personnel should ensure that the fax number is correct for the person or area where the information should be delivered and that the fax number is entered correctly prior to transmission. Once the fax has been sent, the person sending the fax should contact the individual or department to which the information was sent to verify receipt, if this is an individual, department or company to which information is not usually sent. A delivery receipt should be obtained and kept with the documentation as evidence of delivery. If information is delivered to the wrong fax number or successful transmission of a fax cannot be confirmed, the situation is to be immediately reported to the designated Principal.

2.2 Telephone Delivery

When information is to be delivered to the Company by an associated person from an external location via telephone, the individual delivering the information must verify the identity of the person receiving the information by obtaining this person's name and department. If the telephone is not answered, as is generally required by the Company, or the person is unknown to the individual providing the information, the individual should not provide the information and should call back to verify that the number dialed was correct. At no time should information be provided to a person unknown to the deliverer.

Prior to providing information, the individual delivering this information must ensure that the area from which he or she is delivering the information is private and information is not overheard by persons who are not authorized to receive it. Providing non-public information from public areas is strictly prohibited. The recipient of the information must also ensure that no information is repeated if he/she is in a public area or in an area where information may be heard by unauthorized persons.

When providing information to someone over the telephone, the person providing such information must verify the identity of the recipient by asking questions to help identify the person that would not be easily ascertained from identification documents or account information, such as a zip code or the last four digits of their social security number. Information requested will be predetermined by the Company and may include a telephone PIN, the name of the person's pet or some other personal identifying information that cannot generally be obtained from documentation or public records. If the person requesting the information is unable to provide the information requested to identify them, no information may be provided and the designated Principal must be notified immediately. Any breaches to these procedures will result in prompt disciplinary action.

2.3 Electronic Delivery

When information is captured on paper or electronically and is transmitted to the Company via email or other electronic means, the information must be

- Encrypted, and
- Sent only to email addresses authorized by the Company to receive such information.

Under no circumstances can non-public information be stored on portable devices such as PDAs, a thumb/flash drive or laptop unless the information is encrypted and access to the information is protected by a password established under the criteria established by the Company. (See Retention and Back-up below.)

SECTION 3: STORAGE/RETENTION AND BACK-UP

Whenever possible, the Company will seek to minimize the non-public information retained in its files. This can be done through a number of methods, including redacting all but the last 4 digits in a Social Security or credit card number or by not maintaining Social Security, credit card or other identifying numbers. However, the Company may be required to retain non-public information in its files for business or regulatory purposes. In doing so, the Company makes every effort to ensure that the information stored on its systems or in its paper files is secure.

The CCO is responsible for ensuring that the Company's policies related to the retention and storage of non-public information are followed. Should a breach or unauthorized access occur, the designated person identified above must immediately be notified. Failure to provide notification will result in disciplinary action.

The person previously identified shall ensure that any breach, misappropriation or loss of such information is immediately reported to:

- The individual(s) whose information was compromised, and
- Applicable state or federal regulatory or law enforcement agencies.

Failure by the Company to report breaches to files containing non-public information or incidents of identity theft can result in civil and criminal actions against the Company and the persons with knowledge of the breach or theft that did not report it.

3.1 Paper Documents

From the time paper documents containing non-public information are received by the Company, they are maintained in a secure manner. To ensure the confidential retention of such files, the Company has instituted the following procedures:

- All documents being used in work areas must be kept face down when not in use or if the person using the information steps away from his or her work area for a short period.
- All documents not being used for current work processes, or when the person processing the information leaves his or her work area for an extended period, must be locked in file cabinets or desk drawers.
- At the end of the work day, all documents containing non-public information must be removed from work surfaces and stored in locked cabinets containing applicable, related files.
- Only individuals who are required and authorized to receive and access information contained on paper documents may possess those documents or have access to files containing such information.

3.2 Electronic Storage

From the time non-public information is received electronically by the Company, it must be maintained in a secure manner. To ensure the Company's computer systems and files contained thereon are protected from unauthorized access, the following procedures have been adopted:

- Computer systems will be password protected and require multifactor authentication;
- Passwords are confidential and may not be shared with others;
- Servers and desktop computers will be protected through the use of firewall and anti-virus software, which will be set for automatic updates by the vendor to ensure that the most recent versions are maintained;
- Passwords will contain a combination of numbers, letters and/or special characters and be between 6-10 characters in length;
- Systems will automatically block access to users if the login and password combination are incorrect after three successive attempts;
- All files containing non-public information will be encrypted;
- Only persons requiring access to such information will receive access to files containing non-public information; and
- All individuals with access to files containing non-public information will be subject to a background check and fingerprinting.

When accessing files containing non-public information from a remote location, it is important that individuals use only secure connections in private locations or areas. Accessing information over unsecured networks in public locations, such as airports or hotels, can result in that information or those passwords being accessed by unauthorized persons. The Company strictly prohibits persons from accessing non-public information through non-secure networks or in public areas where information can be easily viewed by others.

The CCO will be responsible for maintaining passwords and will be responsible for resetting passwords should access become locked.

Under no circumstances can non-public information be stored on portable devices such as a thumb/flash drive or laptop unless the information is encrypted and access to the information is protected by a password established under the criteria established by the Company. Individuals who wish to maintain information on such devices must obtain permission from the CCO. If such devices are lost or stolen, the incident must be immediately reported to the designated person at the Company so he or she can assess the potential damages and take steps to mitigate risks or report losses as applicable.

SECTION 4: DISPOSAL OR DESTRUCTION OF INFORMATION

Once the Company has terminated the relationship with the individual from whom the non-public information was received or once the Company is no longer required

to maintain such information, it must be disposed of in a manner that ensures that its confidentiality is maintained.

The CCO is responsible for ensuring that the Company's policies are followed relative to the destruction and disposal of paper or electronic files containing non-public information or devices on which such electronic files were stored. Should a breach or unauthorized access occur, the designated person identified above must be notified immediately. Failure to provide notification will result in disciplinary action.

The person previously identified shall ensure that any breach, misappropriation or loss of such information is immediately reported to:

- The individual(s) whose information was compromised, and
- Applicable state or federal regulatory or law enforcement agencies.

Failure by the Company to report breaches to files containing non-public information or incidents of identity theft can result in civil and criminal actions against the Company and the persons with knowledge of the breach or theft that did not report it.

4.1 Paper Files

The Company will ensure all information is protected upon disposal by utilizing an outsourced document destruction company to destroy all paper documents containing non-public information. Supervisors will periodically check offices and trash receptacles to ensure that information is not being disposed of improperly.

4.2 Electronic Files

Simply deleting a file from a computer, a shared server file or portable device does not remove all record of the file. Therefore, the Company will ensure that any files containing non-public information to be removed from computer storage areas are removed by a qualified IT person who will scrub the drive to remove all traces of the files. If the computer or device is to be disposed of, the hard drive will be removed and physically destroyed to ensure that nobody can access any files previously stored on that drive. The Company may periodically contract with an IT professional or service to test the integrity of these procedures by trying to retrieve previously disposed of information from electronic files.

Failure by personnel to dispose of paper or electronic documents, as required by Company policies, will result in immediate disciplinary action.

SECTION 5: USE OF THIRD-PARTY VENDORS

Bates Securities, Inc. makes use of third-party vendors to store or manage customer, employee or other data containing non-public information. These outside vendors are identified in the Company's Written Supervisory Procedures. The relationships with these vendors are the responsibility of the CCO. Bates Securities, Inc. will

ensure that each vendor they utilize that has access to non-public information has systems in place to protect this information and that a confidentiality agreement has been signed. In addition, the Company will require that the vendor provide a certification prior to contracting that outlines the processes and procedures the vendor has undertaken to protect confidential, non-public information, the testing procedures the vendor uses to ensure its systems are functioning properly, and the procedures and timeframes or notification the vendor uses if there are any breaches to these systems. The Company will also require that the vendor certify annually that testing has been undertaken, that no breaches have occurred, and that the firm's systems include the most up-to-date software and hardware for protecting its systems and data store thereon.

SECTION 6: TERMINATION

Upon the termination or resignation of any employee or registered person, the designated manager or supervisor shall secure all keys, files, laptops or other Company property from the individual. At the same, all passwords to Company computer systems used by the applicable person shall be immediately changed. In addition, if the employee or registered person had keys or security passcodes to access Company offices, the locks and/or passcodes shall be changed or disabled to ensure that the individual can no longer access the premises.

Upon the termination of any vendor relation, where the vendor had access to non-public personal information gathered or stored by the Company, the Company shall ensure that all access to such information is terminated and that any information in the vendors possession is immediately returned. Failure of a vendor to return such information will result in a report being filed with the applicable state or federal agency regarding a potential breach.

SECTION 7: TESTING AND DOCUMENTATION

7.1 Testing

At least annually the applicable supervisory personnel at the Company shall evaluate the integrity of the systems and procedures in place to protect non-public personal information gathered by the Company to ensure that, in light of changing business needs, personnel, technology and other matters, the processes and procedures in place continue to meet the needs of the Company and are adequate based on current regulations and the information being gathered and stored.

In addition, the designated managers or principals responsible for the information gathered in various areas of the Company shall conduct reviews of the information security measures being undertaken in their applicable areas of supervision not less than quarterly to ensure that procedures are being followed and the procedures remain adequate based on the current business needs and systems being employed. When needed, changes will be made to the systems or procedures to ensure continuing compliance with applicable State or Federal rules and regulations and the security of non-public personal information gathered and maintained by the Company.

7.2 Documentation

Reviews and remedial action taken, if needed, shall be documented and shall become part of the Company's documentation relating to the annual testing of its policies and procedures

Further, the Company shall maintain records of all potential, suspected or actual breaches including the circumstances surrounding the incident, the action taken to report the breach, if one occurred, and changes made to prevent future breaches.