CONESTOGA CAPITAL ADVISORS, LLC

Privacy Protection, Cybersecurity and Identify Theft Prevention

---

Privacy Protection

Regulation S-P ("Reg S-P") requires registered investment advisers to adopt and implement policies and procedures that are reasonably designed to protect the confidentiality of nonpublic personal records. Reg S-P applies to "consumer" records, meaning records regarding individuals, families, or households.

Reg S-P requires CCA to provide its customers with notices describing the Company's privacy policies and procedures. These privacy notices must be delivered to all new Clients upon inception of an arrangement, and at least annually thereafter.

Cyber Security

The staff of the SEC is concerned by the risk of cyber-attacks against registered investment advisers because of the potential for direct harm against advisers' clients, as well as potential disruptions to market stability that could be intentional or incidental results of a cyber-attack.

Identity Theft Prevention

In addition to Reg S-P and Reg S-AM, the SEC has adopted Regulation S-ID, the "Red Flags Rules," that require certain companies to take steps to detect, prevent, and mitigate the effects of identity theft.

The Red Flags Rules require each SEC registered broker-dealer, investment company, and investment adviser that is a financial institution or creditor to periodically evaluate whether it offers or maintains any covered accounts.

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 an investment adviser to be deemed a financial institution for purposes of the Red Flags Rules include:

- An adviser 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 ; and

- An adviser managing a private fund with one or more natural person investors that permit the adviser or a related person to direct the natural person's redemption proceeds to third parties.

The term "creditor" is defined to include, among other things, any person who extends or arranges credit. A person would not be deemed to be a creditor solely because it bills for services in arrears, or because it advances funds for expenses incidental to the provision of a service. The SEC has stated that an adviser to

a private fund that regularly and in the ordinary course of business lends money to permit individual investors to invest in the fund could qualify as a creditor.

Periodic Assessments

The Red Flags Rules require each investment adviser that is a financial institution or creditor 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 adviser.

The assessment as to whether an adviser maintains any covered accounts must include evaluations of:

- The adviser's method for opening accounts;

- The ways in which clients can access accounts; and

- The adviser's prior experiences with identity theft.

Creating a Written Identity Theft Prevention Program

Any financial institution or creditor that offers or maintains one or more covered accounts must:

- Develop and implement a written Identity Theft Prevention Program (a "Program") that is reasonably designed to detect, prevent, and mitigate identity theft in connection with new and existing covered accounts. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. In particular, the Program must be reasonably designed to:

    - Identify patterns, practices, or specific activities that could be indicative of identity theft ("Red Flags"). Examples of Red Flags are presented in the attachment titled *Examples of Red Flags*;

    - Detect the Red Flags that have been identified by the adviser as potentially applicable;

    - Respond appropriately to any Red Flags that are detected; and

    - Call for periodic updates to reflect any changes in the risks posed by identity theft to the firm or its customers;

- Obtain approval of the initial written Program from the firm's board of directors or an appropriate committee of the board. If the firm does not have a board of directors then approval may be obtained from a designated member of senior management;

- Involve the board, an appropriate committee of the board, or a designated member of senior management in the oversight, development, implementation and administration of the Program;

- Train employees, as necessary, to effectively implement the Program; and

- Ensure that service providers performing activities in connection with one or more covered accounts have their own reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft, and exercise appropriate oversight of those service providers.

As part of the final rule release, the SEC and CFTC issued Program guidelines to assist financial institutions and creditors in the creation and maintenance of a Program meeting the requirements of the Red Flags Rules. These guidelines are described below:

- Consider the following factors when identifying relevant Red Flags:
    - The types of covered accounts it offers or maintains;
    - The methods it provides to open covered accounts;
    - The methods it provides to access covered accounts; and
    - Any previous experiences with identity theft.
- Incorporate relevant Red Flags from the following categories, as applicable:
    - Alerts, notifications, or other warnings from consumer reporting agencies or service providers;
    - The presentation of suspicious documents;
    - The unusual use of, or suspicious activity related to, a covered account; and
    - Notice from customers, victims of identity theft, law enforcement authorities, or others regarding possible identity theft in connection with a covered account.
- Detect Red Flags by:
    - Obtaining identifying information and otherwise verifying the identity of a person opening a covered account; and
    - Authenticating existing customers, monitoring transactions, and verifying the validity of change of address requests.
- Provide for appropriate responses to any Red Flags that are detected. Appropriate responses may include, among other things;
    - Carefully monitoring the affected account(s) for evidence of identity theft or other improper activity;
    - Contacting the affected customer(s);
    - Changing passwords, security codes, or other controls designed to prevent unauthorized access or activity;

- Reopening a covered account with a new account number;
- Not opening a new account, or closing an existing account;
- Notifying law enforcement; and/or
- Determining that an affirmative response is not necessary in light of the relevant facts and circumstances.

- Reevaluate the Program and the risks associated with identity theft at least annually. Such an evaluation should be reflected in a written report that incorporates, as applicable.
  - The firm's experiences with identity theft;
  - Changes in methods of identity theft;
  - Changes in available methods to detect, prevent, and mitigate identity theft;
  - Changes in the types of accounts that the firm offers or maintains; and
  - Changes in the firm's relationships with other entities, such as third-party service providers;

- Oversight by the firm's board of directors, a committee of the board, or a designated member of senior management that includes:
  - Assigning specific responsibility for the Program's implementation;
  - Reviewing reports prepared by employees regarding compliance with the Program; and
  - Approving material changes to the Program as necessary to address changing identity theft risks

- Report to the firm's board of directors, a committee of the board, or a designated member of senior management at least annually on the compliance by the firm with the Red Flags Rules. The report should address material matters related to the Program and evaluate issues such as:
  - Effectiveness of the firm's policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
  - Service provider arrangements;
  - Significant incidents involving identity theft and management's response; and
  - Recommendations for material changes to the Program.

Risks

In developing these policies and procedures, CCA considered the material risks associated with privacy protection and the prevention of identity theft. This analysis included risks such as:

- Nonpublic Personal Information is not recorded accurately or protected from inadvertent alteration or destruction;
- Nonpublic Personal Information is not protected from unauthorized access by Employees or third-party service providers;
- Nonpublic Personal Information can be accessed, copied, or destroyed by physical or electronic intrusions;
- False or misleading disclosures are made to Clients about the use or protection of Nonpublic Personal Information;
- Third-party service providers have adopted inadequate policies and procedures to protect Nonpublic Personal Information;
- CCA fails to comply with applicable state privacy laws applicable to CCA;
- CCA does not identify potential risks to Clients associated with identity theft; and
- CCA does not detect fraudulent attempts to transfer assets out of Client accounts enabled by identity theft.

CCA has established the following guidelines to mitigate these risks.

CCA will not disclose a client's personal information to anyone unless it is permitted or required by law, at the direction of a client, or is necessary to provide CCA's services.

Privacy Protection

Guiding Principles

CCA will seek to limit its collection of Nonpublic Personal Information to that which is reasonably necessary for legitimate business purposes. CCA will not disclose Nonpublic Personal Information except in accordance with these policies and procedures, as permitted or required by law, or as authorized in writing by the Client. CCA will never sell Nonpublic Personal Information.

With respect to Nonpublic Personal Information, CCA will strive to: (a) ensure the security and confidentiality of the information; (b) protect against anticipated threats and hazards to the security and integrity of the information; and (c) protect against unauthorized access to, or improper use of, the information. The CCO is responsible for administering these policies and procedures. Notify the CCO promptly of any threats to, or improper disclosure of, Nonpublic Personal Information.

Although these principles and the following procedures apply specifically to Nonpublic Personal Information, Employees must be careful to protect all of CCA's proprietary information.

Employees will maintain the confidentiality of information acquired in connection with their employment, with particular care being taken regarding Nonpublic Personal Information. Improper use of CCA's proprietary information, including Nonpublic Personal Information, is cause for disciplinary action, up to and including termination of employment for cause and referral to appropriate civil and criminal legal authorities.

All requests by third-parties to review this Manual, compliance testing results, correspondence between CCA and regulators and other compliance-related documents should be forwarded to the CCO. Employees are not authorized to respond to such requests without the prior approval of the CCO.

Procedures

1. CCA shall not sell client information to anyone.

2. CCA will restrict access to clients' personal information to individuals within CCA who require the information in the ordinary course of servicing clients' accounts. Client information is used only for business purposes.

3. CCA has developed procedures to safeguard client records and information (See Attachment A).

4. Client information may only be given to third-parties under the following circumstances:

    - To broker/dealers to open a client's brokerage account;
    - To other firms as directed by clients, such as accountants, lawyers, etc.;
    - To specified family members; and
    - To regulators, when required by law.

5. At times, client information may be reviewed by CCA's outside service providers (i.e. – accountants, lawyers, consultants, etc.). CCA will review the entities' privacy policies to ensure that clients' information is not misappropriated or used in a manner that is contrary to CCA's privacy policies.

6. Prior to providing any third-party service provider with access to personal information about clients who are residents of Massachusetts, CCA will take reasonable steps to verify that such service provider has a written, comprehensive information security program that is in compliance with the provisions of Massachusetts statute 201 CMR 17. The CCO will ensure that any new contracts with such service providers include provisions requiring the service provider's implementation of security policies and procedures that comply with 201 CMR 17.

7. CCA shall provide a privacy notice (See Attachment B) to clients (i.e., "natural persons") upon inception of the relationship and annually thereafter. CCA will maintain a record of the dates when the privacy notice is provided to clients.

8. In the event of a change in the privacy policy, CCA will provide its clients with a sufficient amount of time to opt out of any disclosure provisions.

9. Any suspected breaches to the privacy policy should be reported to the CCO and/or another partner.

10. If an employee receives a complaint regarding a potential identity theft issue (be it from a client or other party), the employee should immediately notify the CCO. The CCO will thoroughly investigate any valid complaint, and maintain a log of all complaints as well as the result of any investigations.

11. In the event that unintended parties receive access to client information, CCA will discuss the matter with legal counsel and promptly notify those clients of the privacy breach as might be necessary. With respect to clients from certain states, this is a specific requirement.

12. Extraneous documents containing any client information or sensitive consumer information shall be burned, shredded or destroyed (this includes documents earmarked for recycling). In addition, any client information saved in a storage medium that is being sold or disposed of, must be removed from the medium.

13. The CCO will ensure that all new employees have received, reviewed, and understand their obligations to protect clients' nonpublic personal information. The CCO will also remind all employees of their privacy protection obligations during the 1st quarter of each year. If the information security/privacy program appears to be functioning well and has not undergone material changes then this reminder might appropriately take the form of a broadly-distributed annual email. The CCO may provide training more frequently and/or in person to individuals or groups if:

    - CCA's policies and procedures, or the threats to clients' nonpublic personal information, change in a material way;

    - CCA experiences a privacy breach; and/or

    - One or more employees do not appear to understand their obligations regarding privacy protection.

14. CCA's premises will be locked outside of normal business hours. The CCO will review the privacy policies and procedures of third-party service providers, such as building custodians, that have access to CCA's facilities. Meetings with Clients should be held in conference rooms or other locations where Nonpublic Personal Information is not available or audible to others.

Cyber-Security Controls Implemented by Information Technology Professionals

The CCO oversees the development and implementation of CCA's cyber-security controls.

On at least an annual basis the CCO will conduct a cyber-security risk assessment with the assistance of CCA's third party information technology service provider. The information technology service providerwill produce a summary of any moderate or high risk vulnerabilities that are identified, as well as a plan to remediate such risks.

Additionally, on an annual basis, CCA will work with the Company's information technology service provider to confirm that CCA has:

- Inventoried its computers, system hardware, and other IT devices such as smart phones;

- Monitored for unauthorized devices accessing CCA's networks;
- Inventoried its software applications, and ensured that software patches are being applied in a timely manner;
- Evaluated likely types of attack, including through penetration testing and vulnerability scans, where appropriate;
- Implemented appropriate protections, such as anti-malware software, firewalls and data loss prevention software;
- Tested CCA's ability to restore critical data and software in a timely manner;
- Implemented standardized secure configurations for user hardware, software, operating systems, and network infrastructure;
- Periodically tested to confirm that hardware, software, operating systems and network infrastructure continue to operate according to their standardized secure configurations;
- Appropriately tested software applications prior to implementation;
- Encrypted any wireless data transmissions in CCA's offices that could contain sensitive data;
- Mapped its network resources, and ensured that CCA has appropriately limited access to drives and applications that host sensitive data;
- Mapped external access points to CCA's network;
- Evaluated the cyber-security programs of vendors or other third parties that have independent access to CCA's networks or proprietary data, and, where appropriate, ensured that third party contracts or statements of work include appropriate provisions governing cyber-security;
- Implemented adequate access logging capabilities, as well as automated exception reporting capabilities that are reasonably designed to detect malicious activity;
- Promptly disabled access for any terminated Employees; and
- Permanently erased or destroyed any electronic storage media that is being discarded.

Responding to Privacy Breaches

If any Employee becomes aware of an actual or suspected privacy breach, including any improper disclosure of Nonpublic Personal Information, that Employee must promptly notify the CCO. Upon becoming aware of an actual or suspected breach, the CCO will investigate the situation take the following actions, as appropriate:

- To the extent possible, identify the information that was disclosed and the improper recipients;
- Notify appropriate members of senior management;

- Take any actions necessary to prevent further improper disclosures;
- Take any actions necessary to reduce the potential harm from improper disclosures that have already 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 Clients, and make any such notifications;
- Collect, prepare, and retain documentation associated with the inadvertent disclosure and CCA's response(s); and
- Evaluate the need for changes to CCA's privacy protection policies and procedures in light of the breach.

Privacy Protection Training

The CCO will ensure that all new Employees have received, reviewed, and understand their obligations to protect Nonpublic Personal Information. The CCO will also remind all Employees of their privacy protection obligations during the first quarter of each year. If the Program appears to be functioning well and has not undergone material changes then this reminder might appropriately take the form of a broadly-distributed annual email. The CCO may provide training more frequently and/or in person to individuals or groups if:

- CCA's policies and procedures, or the threats to Nonpublic Personal Information, change in a material way;
- CCA experiences a privacy breach; and/or
- One or more Employees do not appear to understand their obligations regarding privacy protection.

Identity Theft Prevention Program

The CCO, who is a member of senior management, was involved in the preparation of CCA's Identity Theft Prevention Program (the "Program") and is responsible for overseeing the Program's implementation. In creating this Program, the CCA considered, among other things:

- The types of accounts that CCA manages;
- The scope and nature of CCA's relationships with Clients and prospects;
- CCA's processes for opening and closing accounts and for accessing accounts;
- CCA's prior experience with identity theft;

- Other industry participants' experiences with identity theft, including perceived changes in the methods used to engage in identity theft; and

- Regulatory guidance issued by the SEC.

Identity Theft Risk Assessment

CCA has determined that the risks associated with identity theft to the Company and its Clients is low because:

- CCA provides personalized services to a relatively small number of Clients;

- CCA often meets with Clients in person;

- All Client assets are held by reputable Qualified Custodians. For Client accounts where CCA serves as trustee, CCA does not typically initiate or process payments to third parties form these accounts; and

- CCA has never experienced an incidence of identity theft.

Identifying Red Flags

CCA has carefully considered the types of events that could be Red Flags for identity theft. It is not possible to identify every potential Red Flag in advance, so Employees should consult with the CCO if there is any question as to whether a development may be indicative of identity theft. The following list is meant to identify the events that the Company believes possess the greatest likelihood of being indicative of identity theft, given the scope and nature of CCA's operations.

- A notification from a Client or prospect that the individual was the victim of identity theft;

- A fraud alert or other communication about identity theft from a government official, including a law enforcement officer, a Qualified Custodian, a consumer reporting agency, or service providers, such as fraud detection services;

- Mail from CCA to a Client or prospect that is returned to the Company as undeliverable;

- Requests or behavior by a Client or prospect that are materially different from the individual's past requests or behavior;

- Account changes or transaction requests that do not appear to serve a legitimate economic purpose;

- Unanticipated capital transfers that are large and/or frequent;

- Documents that are incomplete or appear to have been altered or forged;

- The provision of inconsistent information on forms or during conversations; and

- An unwillingness to participate in normal processes that CCA uses to establish and maintain Client relationships.

Detecting Red Flags

CCA has adopted the following policies and procedures that are designed to detect potential indications of identity theft, including the Red Flags described above:

- All Employees have been trained to promptly inform the CCO of any communications regarding identity theft. Employees understand that such communications may be oral or in writing, and may come from Clients, prospects, government officials, law enforcement officers, custodians, and consumer reporting agencies, among others.

- All Employees have been trained to promptly inform the CCO of any mail sent to Clients or prospects that is returned as undeliverable.

- Clients and prospects interact repeatedly with CCA's Employees. These repeated interactions put CCA's Employees in a good position to detect the provision of inconsistent information, an unwillingness to share routinely gathered information, or any material changes in behavior. Employees have been trained to promptly inform the CCO of any suspicious activities.

- CCA is generally familiar with each Client's financial objectives, as well as the source and scale of each Client's wealth, so account changes or transaction requests that do not serve a legitimate economic purpose would be apparent. Employees have been trained to promptly inform the CCO of any suspicious account changes or transaction requests.

Responding to Red Flags

As noted previously, Employees have been trained to promptly notify the CCO of any apparent Red Flags. Upon becoming aware of a Red Flag, the CCO will investigate the situation and consider taking one or more of the following actions:

- Carefully monitoring the affected account(s) for evidence of identity theft or other improper activity;

- Contacting the affected customer(s);

- Changing passwords, security codes, or other controls designed to prevent unauthorized activity;

- Reopening a covered account with a new account number;

- Not opening a new account, and/or closing an existing account;

- Not attempting to collect on a covered account or not selling a covered account to a debt collector;

- Notifying law enforcement;

- Changing the Program; and/or

- Some other appropriate response, including determining that no response is warranted under the particular circumstance.

The CCO will seek to respond in a manner that is appropriate given the relevant facts and circumstances. The CCO may consult with other Employees, ACA Compliance Group, and/or Outside Counsel when determining the appropriate response to a Red Flag. In certain circumstances the CCO may determine that no response is necessary or appropriate.

Review and Oversight of the Program

CCA will review the Program during the first quarter of each year. This review will be overseen by the by the CCO who is a member of senior management and will include, as applicable, an evaluation of:

- CCA's compliance with the Program;
- CCA's experiences with identity theft;
- Changes in methods of identity theft;
- Changes in available methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts that CCA offers or maintains;
- Service provider arrangements
- Changes in CCA's relationships with other entities, including affiliates, joint ventures, and third-party service providers; and
- Any recommended changes to the Program.

CCA will document its annual reviews of the Program in writing; the CCO will be responsible for retaining all such documentation. Should any material issues be identified a report addressing the specific issues identified will be provided to each member of senior management.

issues material matters related to the Program and evaluates issues, including but not limited to:

- Effectiveness of the firm's policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
- Service provider arrangements;
- Significant incidents involving identity theft and management's response; and
- Recommendations for material changes to the Program.

Red Flags Training

The CCO will ensure that all new Employees have received, reviewed, and understand their obligations under this Program. The CCO will also remind all Employees of their obligations under the Program during the firstquarter of each year. If the Program appears to be functioning well and has not undergone material changes then this reminder might appropriately take the form of a broadly-distributed annual email. The CCO may provide training more frequently and/or in person to individuals or groups if:

- The Program, or the risks associated with Red Flags, changes in a material way;
- CCA is affected by an incidence of identity theft; and/or
- One or more Employees do not appear to understand their obligations under the Program.

The CCO will document training given to new and existing Employees about the Program.

Address Changes

Employees may only process an address change on behalf of a Client after confirming the identity of the requestor. Confirmation could be achieved over the phone if an Employee has a close relationship with the Client, but written authorization should be obtained if there is any question as to the identity of the requestor.

In all instances, the CCO will confirm a change of address by sending letters to the new and old addresses of record.

Responsibilities

The CCO will monitor for compliance with CCA's Privacy Policy and Name will coordinate the dissemination of the Privacy Notice. The CCO will use a *Privacy Protection Training Log* (See Attachment C) to document training given to new and existing employees.

Attachment A

Procedures to Safeguard Client Records and Information

CCA shall (a) ensure the security and confidentiality of consumer, customer and former customer records and information; (b) protect against any anticipated threats or hazards to the security or integrity of consumer, customer and former customer records and information; and (c) protect against unauthorized access to or use of consumer or customer records or information that could result in substantial harm or inconvenience to any customer. Accordingly, the following procedures will be followed:

A. **Desktop Computer Security and Cybersecurity Guidelines**.

1. Definition

Desktop computers are personal workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units.

2. Hardware Security

a) Lock main office. The office keys should be monitored to ensure they are returned when an employee leaves CCA.
b) Locate computers away from environmental hazards.
c) Follow standard data backup procedures.

3. Access Security

a) Utilize password facilities to ensure that only authorized users can access the system. Where the Desktop is located in an open space or is otherwise difficult to physically secure, consideration should be given to enhanced password protection mechanisms and procedures.
b) Password guidelines:

- Length should be eight characters. (Six-character passwords may suffice for non-dictionary words.)
- Avoid words found in the dictionary and include at least one numeric character.
- Choose passwords not easily guessed by someone acquainted with the user. (Passwords should not be maiden names, or names of children, spouses, or pets.)
- Do not write passwords down anywhere.
- Change passwords periodically.
- Do not include passwords in any electronic mail message.

c) Password guidelines: Employees must never share their passwords or store passwords in a place that is accessible to others;

d) Employees must shut down or lock their computers when they leave the office for any extended period of time;

e) Any inquiries or requests for representations about CCA's cyber-security controls from third parties, such as Clients, Investors, vendors, or government officials, must be forwarded to the CCO.

f) Any requests from third parties for independent access to CCA's networks or proprietary data must be forwarded to the CCO. Only the CCO may respond to such access requests.

B. The CCO is responsible for setting Employees access permissions on the Company's computer network.

1. Data and Software Availability

a) Back up and store important records and programs on a regular schedule.
b) Check data and software integrity.
c) Fix software problems immediately.

2. Confidential Information

a) Encrypt sensitive and confidential information where appropriate. Employees must not include Nonpublic Personal Information in unencrypted emails sent outside of CCA's network;
b) All laptops and portable storage devices containing nonpublic personal information about residents of Massachusetts must be encrypted.
c) Monitor printers used to produce sensitive and confidential information.
d) Overwrite sensitive files on floppy disks and CDs.
e) Any theft or loss of electronic storage media must immediately be reported to the CCO;
f) Employees must consult with the CCO before using any removable or mobile media to store sensitive CCA data, including Nonpublic Personal Information.
g)

3. Viruses

Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource

environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.

To decrease the risk of viruses and limit their spread:

a) Check all software before installing it.
b) Use software tools to detect and remove viruses.
c) Isolate immediately any contaminated system.

4. Computer Networks

Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks. While CCA has the responsibility for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating their own computer with ethical regard for others in the shared environment. The following considerations and procedures must be emphasized in a network environment:

a) Check all files downloaded from the Internet. Avoid downloading shareware files.
b) Test all software before it is installed to make sure it doesn't contain a virus/worm that could have serious consequences for other personal computers and servers on the Firm network.
c) Choose passwords with great care to prevent unauthorized use of files on networks or other personal computers.
d) Always BACK-UP your important files.
e) Use (where appropriate) encrypting/decrypting and authentication services to send confidential information over the Internet.

C. **Physical Data Security Guidelines**

1. During working hours, authorized personnel must occupy the area where we maintain or regularly use nonpublic client information or restrict storage of such information to locked metal file cabinets or a locked room. During nonworking hours, nonpublic personal information should be stored in a locked room. Where the locked room is the system of security, no master key should be available. A master key opens rooms other than the room containing the nonpublic personal information. Where the locked room contains records accessible by unauthorized individuals, separate the records into individual locked file cabinets.

2. If your duties require handling nonpublic personal information, you must always take care to protect the integrity, security, and confidentiality of these records. Do not put papers containing nonpublic personal information into the recycle bins or trash receptacles (e.g., client lists, account statements, tax returns). Confidential material should be shredded.

Attachment B

Privacy Notice

CONESTOGA CAPITAL ADVISORS LLC
NOTIFICATION OF PRIVACY POLICIES AND PRACTICES

Maintaining the confidentiality of the personal information of our current and prospective clients is one of our highest priorities. This notice sets forth the type of personal information we collect, how that information is used by us, and how we protect your personal information.

Information We Collect

Personal information is collected from you in order to offer or provide you with products or services, process transactions on your behalf, and comply with legal and regulatory requirements.

Information may be collected from any of the following sources.

From You: Your personal information is collected and maintained by us so we may develop, offer, and deliver products and services to you, process transactions in your account, and fulfill our legal and regulatory requirements. We collect information from you when you enter into an advisory agreement with our firm, seek advice about investments, tell us about your investment portfolio, complete account opening forms, and provide contact information. This information may include items such as your name, address, email address, social security number, birth date, annual income, assets, investment experience, account balances, transaction history and risk tolerances.

From Transactions: If you obtain advice or services from us, we keep records of the advice or services provided. We keep records relating to items such as your account balances and transaction history which enables us to resourcefully service your account.

From our Web Site: If you visit our website, we may use a so-called cookie to track the amount of time you spend on our site, the parts of our site you visited, and other technical information. We use this information to improve the functionality of our web site.

Information We Disclose

We do not disclose any non-public personal information about our investors or former investors to anyone, except as permitted or required by law, or as necessary to provide services to you. We may disclose all of the information we collect, as described above, to certain non-affiliated third parties such as, but not limited to, fund administrators, attorneys, accountants, compliance consultants, and persons or entities to enable us to provide requested services to you and to comply with legal and regulatory requirements.

Protection of Your Personal Information
Our employees may, from time to time, have access to your personal information in order to provide services to you. All employees are subject to the terms of our company's compliance manual, which requires employees to treat confidentially all information obtained from or about you or your account. We also maintain physical, electronic, and procedural safeguards designed to protect nonpublic personal financial information.

Attachment C

Privacy Protection/Identity Theft Training Log

Training Recipient(s)	Training Description	Date Provided	Provided by