

# CONESTOGA CAPITAL ADVISORS, LLC

## Policy

### Client Privacy

---

#### Issue

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 investment advisers to disclose to clients its policies and procedures regarding the use and safekeeping of personal information.

Personal 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 a high level of service.

While CCA strives to keep client information up to date, clients are requested to monitor any information provided to them for errors.

#### Policy

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.

#### 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. 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.

7. 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.
8. Any suspected breaches to the privacy policy should be reported to the CCO and/or another partner.
9. 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.
10. 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.
11. 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.

### **Responsibilities**

The CCO will monitor for compliance with CCA's Privacy Policy and will coordinate the dissemination of the Privacy Notice.

## 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 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.

##### 4. 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.

##### 5. Confidential Information

- a) Encrypt sensitive and confidential information where appropriate.

- b) Monitor printers used to produce sensitive and confidential information.
- c) Overwrite sensitive files on floppy disks and CDs.

6. 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.

7. 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.

**B. 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.

### C. **Identity Theft**

1. An identity thief can obtain a victim's personal information through a variety of methods. Some of these methods are directly related to CCA and industry practices that put consumers at risk. Employees should be aware of how their actions may expose our clients to the dangers of identity theft.
2. Employees should take the following actions to prevent identity theft:
  - a) When providing copies of information to others, employees should make sure that nonessential information is removed and that nonpublic personal information that has no relevance to the transaction is either removed or masked.
  - b) The practice of *dumpster diving* provides access for a would-be thief to a client's personal information. If you discard papers containing personal client identification information without shredding the documents, a thief may retrieve this information from our waste management facilities. Therefore, when disposing of paper documents, the papers should be shredded.
  - c) To help prevent a fraudulent address change, verify requests before executing them. Send confirmation of address changes to both the new and the old address of record.
  - d) CCA's employees may also be deceived by *pretext calling*, defined as an information broker or identity thief calling CCA while pretending to be a client, and may even use bits of a client's personal information (such as a Social Security Number) to maintain the deception. The information thief convinces the employee to provide additional information over the phone, which can be used for fraudulent purposes. Employees should make absolutely certain that they confirm the identity of the client on the phone before divulging personal information.
  - e) CCA prohibits the display of Social Security Numbers on any documents that are widely seen by others (e.g. client files, mailing lists, quarterly reports, etc.).
  - f) Employees may be responsible for identity theft through more direct means. Insider access to information allows a dishonest employee to sell consumers' personal information or to use it for fraudulent purposes. Such action is cause for immediate termination of employment and may subject the employee to civil and criminal liability.

## **Attachment B**

### **Privacy Notice**

This notice is being provided to you in accordance with the Securities and Exchange Commission's rule regarding the privacy of consumer financial information ("Regulation S-P"). Please take the time to read and understand the privacy policies and procedures that we have implemented to safeguard your nonpublic personal information.<sup>1</sup>

#### **INFORMATION WE COLLECT**

Conestoga Capital Advisors, LLC must collect certain personally identifiable financial information about its customers to ensure that it offers the highest quality financial services and products. The personally identifiable financial information which we gather during the normal course of doing business with you may include:

1. information we receive from you on applications or other forms;
2. information about your transactions with us, our affiliates, or others;
3. information collected through an Internet "cookie" (an information collecting device from a web server); and
4. information we receive from a consumer reporting agency.

#### **INFORMATION WE DISCLOSE**

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law. In accordance with Section 248.13 of Regulation S-P, we may disclose all of the information we collect, as described above, to certain nonaffiliated third parties such as attorneys, accountants, auditors and persons or entities that are assessing our compliance with industry standards. We enter into contractual agreements with all nonaffiliated third parties that prohibit such third parties from disclosing or using the information other than to carry out the purposes for which we disclose the information.

#### **CONFIDENTIALITY AND SECURITY**

We restrict access to nonpublic personal information about you to those employees who need to know that information to provide financial products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.

---

<sup>1</sup> Nonpublic personal information means personally identifiable financial information and any list, description or other grouping of consumers that is derived using any personally identifiable financial information that is not publicly available.

# CONESTOGA CAPITAL ADVISORS, LLC

## Policy

### Duty to Supervise

---

#### Issue

Section 203(e) of the Advisers Act states, in part, that the SEC may prohibit investment advisers from engaging in investment advisory activities for a period not exceeding twelve months, or in the worst case scenario, revoke the registration of the investment adviser. The severity of the sanction is determined on a case-by-case basis; however, past SEC enforcement actions have observed the reasonableness of compliance procedures as an affirmative defense against a claim of failure to supervise.

CCA's management recognizes its duty to supervise the actions of its employees. The Code of Conduct and Regulatory Compliance Manual assists management in carrying out this task by providing guidance in completing advisory activities and setting forth the ethical issues to be considered by the firm. CCA shall carefully review the following activities (note that this list is not all-exhaustive):

- Setup of new accounts
- Securities pricing and valuation
- Preparation of investment advisory agreements
- Maintenance of client files
- Portfolio management
- Client trading, including best execution and trade allocations
- Customer correspondence
- Personal trading activities of employees
- Customer complaint inquiries
- Form ADV amendments
- Regulatory registration issues
- Marketing and advertising
- Adherence to the Code of Conduct

#### Policy

CCA's officers will reasonably supervise the activities of its employees.

#### Procedures

Supervision over certain responsibilities is generally delegated to various employees within CCA. Such delegation of responsibilities must occur to ensure that CCA provides clients with the highest level of service. CCA operates within a well-defined supervisory structure that outlines the responsibilities of its employees and the individuals to whom they report.

CCA expects that its employees will report to their supervisors any issues arising in which they may be unfamiliar or may otherwise require the assistance and judgment of senior management. Employees must also report any activities that run contrary to the Code of Conduct and that may adversely affect the reputation of CCA. An employee may report suspicious activity anonymously to the Chief Compliance Officer, the Deputy Compliance Officer, the compliance consultant to CCA, Counsel to CCA or Counsel

to the Conestoga Funds. All activities reported by employees shall be investigated by the Chief Compliance Officer or in certain cases by the compliance consultant, Counsel to CCA, or Counsel to the Conestoga Funds without revealing the identity of the reporting employee to any member of management in order to protect the reputations of the employees involved. CCA shall commit to a full unbiased review of the matter and implement the necessary corrective and disciplinary action. CCA requires the full commitment of its employees to the tenets set forth in the Code of Conduct; employees that elect to ignore and/or violate the tenets shall be disciplined as such including the possible termination of their employment with CCA.

### **Responsibilities**

CCA employees with supervisory responsibilities are required to supervise the activities of their subordinates and report any material issues to a partner of CCA.