OM FINANCIAL INC.
A Company With a ♥!

PRIVACY PROGRAM

Revised: July 18, 2023

The Personal Information Protection and Electronic Documents Act ("PIPEDA") applies to all organizations, including Insurance Producers, engaged in commercial activities across Canada, except in those provinces that have substantially similar laws. PIPEDA also applies to the *federally regulated* private sector regardless of where situated and to personal information ("PI") in inter-provincial and international transactions. Because virtually all insurers with which insurance Producers do business are federally regulated, the *customer* information you collect, use and retain on behalf of insurers or on behalf of your customer is subject to PIPEDA. The information MGAs collect on Producers as part of their screening and monitoring is protected by PIPEDA or by substantially similar provincial regulation.

PIPEDA applies to *employee* information *only* in organizations that are engaged in federal works, undertakings or businesses, such as most insurers. Because Producers are provincially licensed and regulated, provincial laws govern personal information you might collect on employees.

See "Contact Information" at the back of this section for information regarding federal and provincial contacts.

PRIVACY POLICY

At OM Financial Inc., we are committed to protecting the confidentiality and security of our advisors, clients, insurance providers, and employees' personal information. Our Privacy Policy sets out our standards in collecting, using, disclosing, and retaining your personal information.

Definition of Personal Information:

Personal Information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form such as:

- Age, name, ID numbers, income, ethnic origin, DNA or blood type;
- Opinions, evaluations, comments, social status, or disciplinary actions; and
- Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (i.e., to acquire goods or services, or change in jobs)

A Summary of PIPEDA

An individual's consent must be taken to collect, use or disclose the individual's personal information("PI"). An individual has a right to access PI we hold on them and to challenge its accuracy. PI can only be used for the purposes for which it was collected. If we wish to use it for another purpose, we must obtain consent again. We also need to assure individuals that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.

Complaints: An individual may complain to us or the OPCC about any alleged breaches of the law. The OPCC may also initiate a complaint if there are reasonable grounds.

Application to the Federal Court: After receiving the OPCC's investigation report, a complainant may apply to the Federal Court for a hearing under certain conditions set out in the Act. The OPCC may also apply to the Court, which can order us to change our practices and/or award damages to a complainant, including damages for humiliation suffered. We reserve the right to contact our legal counsel for advise

and direction.

Audits: With reasonable grounds the OPCC may audit our PI management practices.

Offences: OM Financial Inc. acknowledges that it is an offence to:

- destroy PI that an individual has requested.
- retaliate against a covered employee who has complained to the OPCC or who refuses to contravene Sections 5 to 10 of the Act; or
- Obstruct a complaint investigation or an audit by the OPCC.

Provincial Privacy Laws – Variations

Currently Alberta, Quebec and British Columbia have substantially similar privacy laws. Ontario has enacted a law that is substantially similar in its treatment of personal health information. The OPCC, Alberta and British Columbia have signed a memorandum of understanding, in an effort to collaborate and cooperate in their approaches to regulation.

Alberta's law, known as "PIPA" is virtually identical to PIPEDA and is complaint-driven like PIPEDA. The Alberta Privacy Commissioner has more latitude than is allowed for under the federal act, but Alberta tries to resolve disputes through fact-findings, mediation and education.

The **BC** Act (also known as "PIPA) differs from the Alberta Act with respect to enforcement powers. The BC Privacy Commissioner has express audit powers, but the orders of the BC Commission do not become orders of the Court, as they can in Alberta and Quebec.

The **Quebec** Act, known as "An Act Respecting the Protection of Personal Information in the Private Sector," reflects the fact that privacy is a right guaranteed by Quebec's Charter of Rights and Freedoms. Damages can be sought in the courts and violations of the Act are punishable by significant fines. However, like Alberta and BC, Quebec attempts to mediate disputes first.

Ontario's Personal Health Information Protection Act is substantially similar to PIPEDA in its treatment of health information. PIPEDA applies in all other respects in Ontario. Protection of employee information, other than in federally regulated endeavors, represents a gap.

Also note that some provinces have rules relating to personal information that is sent outside of province. You should become familiar with the privacy laws in the provinces in which you operate.

Insurers and MGA Contractual Requirements

IMPORTANT NOTE:

We gather, use, and retain information about our customers for submission to insurers in order todetermine their needs and identify suitable products and recommendations. We do this on our own behalf. When we pass some or all this information through to the insurer on an insurance application, we generally do this on behalf of the insurer pursuant to a written contract. However, not all insurers include MGAs in their consents in their applications and forms. Because we likely collect more information than we submit on an application, we must ensure that we have the customer's explicit writtenconsent to collect, use and retain the information. Furthermore, because producers may use MGAservices that are not explicitly covered by the consent's insurers attach to their applications (e.g., general marketing support), we must ensure that the written consent we receive from the customer includes consent to share PI with us.

OM FINANCIAL INC.
A Company With a ♥!

PIPEDA's 10 Principles – Our Responsibilities and How we Comply

PIPEDA incorporates the 10 principles of Canadian Standards Association's *Model Code for the Protection of Personal Information* and imposes certain responsibilities on MGAs and Producers regarding how they handle customers' personal information in their possession. Our Privacy Policy is designed for advisors, so that they understand how we manage their personal information as well as that of their customers.

Principle 1: Accountability

We are responsible for your personal information in our possession or control. Our Privacy Officer monitors compliance with the Privacy Policy we have set in place.
Access to personal information is limited to those who have viewing authorization.
OM Financial Inc. will comply with the laws and regulations applicable in all jurisdictions; PIPEDA in Canada, ALPIPA in Alberta, BCPIPA in British Columbia.

Principle 2: Identify Purpose for Collection

We collect personal information for the purpose of the following:

- Documenting files.
- Assessing your financial needs.
- Confirming identity and accuracy of information provided.
- Protecting you and us against fraud.
- Submitting applications.
- Opening accounts.
- Meeting legal and regulatory requirements.
- Providing you with ongoing information about new products and services offered
- Maintaining communication.
- Complete requested transactions.
- Disclosing any missed information for a policy application to an insurance company.

We act as an intermediary between insurance brokers and AGAs and the insurance companies with which they do business, contracted by insurers to operate on their behalf to facilitate sales and support of life and health insurance and investment products. Insurers' privacy policies sometimes identify us as "service providers." Insurers require us to obtain, use and retain certain essential personal information about Advisors to determine their initial and ongoing suitability to act as an advisor, to obtain contracts for them to distribute products and to compensate them. This information includes financial and work history as well as disciplinary, legal, and regulatory information.

We obtain customer information from Advisors to provide services and access to insurers' products. Our policies must meet the standards insurers' establish. The personal information advisors collect from customers and provide to us for submission to insurers are essential information that insurers use to provide services and products that customers have requested. This information is used to determine insurance risk, assess eligibility for products, to administer those products once purchased and to fulfill certain regulatory requirements.

Principle 3: Consent

Before obtaining any personal information from you, we require your consent to collect, use, and disclose information for the purpose we specify as well as when a new use or adjustment of your personal information is required.
You may deny us or withdraw your consent to the use and disclosure of your personal information, subject to legal or contractual restrictions. However, we will advise you that if you choose to withhold required information, we may be unable to provide necessary recommendations and services that would be best suited

to your needs.

Principle 4: Limiting Collection

We collect only the information we need to fulfill our contracts with advisors and insurers and to meet our regulatory obligations. We will use only fair and lawful means to collect this information. We collect personal information to provide you with high quality services. Personal information that we collect includes, but not limited to:

- Name
- Contact information
- Occupation
- Income
- Citizenship Status
- Credit information
- Financial information
- Health information
- Marital status
- Date of Birth
- Gender
- Social Insurance Number

Principle 5: Limiting Use, Disclosure, and Retention

Access to your personal information is limited to those who are authorized, only to the extent necessary to perform their duties.

Necessary Information Disclosure:

Personal information to third parties may be disclosed in the following situations:

1. To process authorized transactions, to secure insurance quotations, to acquire insurance coverage, and/or to report or process transactions for other parties that perform services on our behalf.
2. Personal information may also be disclosed to a third party, as the law stipulates, when a portion or all of our business is sold to a company, or pursuant to a subpoena, court order, or other litigation that forces information to be disclosed.

Personal information shall be retained only for as long as needed to fulfill the purposes for which it was collected. Two exceptions to this requirement are (i) if the individual consents to a longer retention period, or (ii) if longer retention is required by law. Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous.
Advisors should consider any provincial regulation or guidance which may prescribe longer retention period, but in general should not destroy information for at least 7 years after the insurance contract has ended or closed. This is to ensure OM Financial Inc.'s and our advisors are in compliance with PIPEDA.

Principle 6: Accuracy

It is the Advisor's responsibility to keep the personal information we obtain about the advisor and customer as accurate and up-to-date as possible. Both the insurer and the advisor are responsible for providing us with notices of changes that they receive directly. An individual may challenge the completeness and accuracy of his/her personal information that we hold. We will make necessary corrections to information about an advisor that is shown to be incomplete or inaccurate and we will notify any third parties, including insurers, if we agree to make such corrections.

Customers may gain access to their personal information we hold by making an access request to the Advisor and/or insurer on whose behalf we hold the information. In situations where a customer seeks corrections to information we hold, we will act on the instructions of the insurer(s) whose products are held and/or the Advisor who is their authorized representative, depending on the corrections required. Any disagreement or discrepancy regarding accuracy will be documented.

Principle 7: Safeguards

OM Financial Inc. has an Internal Office Privacy Policy, implemented in both Toronto and Mississauga locations. We protect personal information against loss or theft by keeping physical files in locked cabinets and limiting its access to authorized personnel. We implement security measures in the office by providing building accesscard to employees, visitor identification registration, etc.
Technologically, we use safety measures such as logins, passwords, and encryption.

File Management

- Client accounts are segmented into separate files on Virtgate unless the policy is a joint one.
- Files for insurance and securities business are uploaded on Virtgate. Accounts are created for each client. If client has both insurance and securities business, separate accounts are created for each businesses.

Principle 8: Openness

OM Financial Inc. understands that:

- They must inform individuals that they have policies in place for managing personal information.
- They must make the updated Privacy Policy understandable and easily available through our website.

Principle 9: Individual Access

You have the right to see the personal information we have of you on file as well as how it is used and disclosed. To do so, you will need to send a written request by email or mail to our Privacy Officerusing the address found below.

Principle 10: Complaints and Concerns

You may contact us with any concerns, questions, and suggestions with respect to our ten privacy principles. Each complaint received will be recorded in our Complaint Investigation Log.

Privacy Officer
Rahul Bharadwaj
Email: president@omfinancial.com
Tel: (416) 491-7727 ext: 223
Fax: (905) 612-0801
Office Address:

Toronto
7191 Yonge Street Suite #711
Thornhill, ON, L3T 0C4

Mississauga
218 Export Blvd
Suite 610
Mississauga, ON L5S 0A7

OM FINANCIAL INC.
A Company With a ♥!

The Compliance Program

The OPCC indicates that the Privacy Compliance Officer ("PC Officer") needs the authority to intervene on privacy issues relating to any of your work. In particular, this person must have the ability to respond to investigators, auditors and the OPCC. OM Financial Inc. has a Compliance and Privacy officer as mentioned below. In most cases, the Producer will be the Compliance Officer.

OM Financial Inc. overall privacy affaires are handled by **Rahul Bhardwaj.**

Receiving and processing access requests - the Rules

It is expected that access requests will be relatively rare.

Any customer information producer obtain that is required by the insurer for issuance of a policy is collected under the insurer's consent. Any additional information that producer obtain, which is not passed through to the insurer, must be collected under a consent that producer obtain directly from the customer. This includes needs analyses and any other information that relates to producer relationship as an advisor or financial planner with the customer. When producer receive an access request from a customer, Producer must determine whether the information requested was collected on behalf of the insurer or for their own practice. If a customer wishes to access the needs analysis only, the Producer will have to respond to the request. Realistically, any access request will be more general and will involve information collected on behalf of both insurer and Producer. In contacting both OM Financial Inc. and insurer, from time-to-time producer or OM Financial Inc. may be asked to respond. Either way, written instructions from both parties is advisable.

The following rules apply:

1. The response to a customer's access request must be made within 30 days. This can be extended for a maximum of 30 additional days, if:

    - responding to the request within the original 30 days would unreasonably interfere with the parties' activities.
    - More time is necessary to conduct consultations or to convert PI to an alternate format.

2. If a time extension is needed, the individual must be notified within 30 days of receiving the request, and of his or her right to complain to the OPCC.

3. Assistance must be provided to any customer who needs to prepare a PI request.

4. The individual may be asked to supply enough information to enable the parties to account for the existence, use and disclosure of PI.

5. Access must be provided at minimal or no cost to the individual.

6. The individual must be notified of the approximate costs before processing the request and asked to confirm that the individual still wants to proceed with the request.

7. The requested information must be understandable, and acronyms, abbreviations, and codesmust be explained.

8. The parties must send any information that has been amended, where appropriate, to any 3rd

parties that have access to the information. This includes OM Financial Inc.

9. The individual must be informed in writing when an access request is refused, setting out the reasons and any recourse available.

Customer Access Requests –*Procedures* - If we receive a request directly from a customer:

1. Be careful not to help the customer "crystallize" a complaint. Ask questions but will not attempt to write their concerns for them.

2. Anyone, including the advisor, making a request on someone else's behalf needs written authorization from the owner of the PI.

3. Notify OM Financial Inc. PC Officer of the request, who will likely notify the insurer(s)' contact person directly and ask for written instructions as to whether they will handle the request or require us to be involved. OM Financial will require instructions on handling any PI in their possession, including whether the information needs to be provided in a certain format, the deadlines for providing the information, etc.

Advisor Access Requests: Requests for your own PI must be directly to OM Financial Inc.'s PC Officer.

Receiving and Responding to Inquiries and Customer Complaints –procedures:

If OM Financial Inc. receives a privacy-related complaint directly from a customer, we will take the following actions:

1. Get the facts and attempt to resolve the complaint immediately, if that is possible. At the same time, we are careful not to assist in forming the complaint, as this often "crystallizes" a complaint in a manner that the individual never intended.

2. OM Financial Inc. PC Officer should be notified immediately, who may:

   - notify the insurer(s) involved and ask for written instructions if OM Financial Inc. assistance is required in providing PI or resolving the complaint;
   - ask to be kept apprised so that you any necessary changes to policies and procedures can be made and the complaint can be closed off in our complaint log.

Safeguarding information

How we safeguard PI is very likely the most critical element of our privacy efforts, given the sensitive nature of information that producers collect directly and indirectly, which we use and retain.

OM Financial Inc. has appropriate safeguards to ensure that PI is protected from loss, theft and inadvertent destruction, among other things.

PI owned by customers is maintained in paper and electronic format in our office and producer offices. We have the following controls in place to safeguard this information:

Physical Safeguards – OM Financial Inc. ensure that branches at Toronto and Mississauga aresecure through use of:

- Locks
- Alarms

- Fire suppression
- Access keys
- Paper files holding PI are kept in locked file cabinets
- Reception areas

Operational Safeguards

You have:

- A clean desk policy.
- Policies and procedures regarding information security.
- Policies and procedures regarding access to PI in work-at-home arrangements.
- Record retention and destruction schedules
- Prohibit the removal of PI from our offices.
- We train staff on information security and the need to safeguard PI.
- We provide access to PI on a need-to-know basis, generally based on the roles that staff performs.
- We regularly backup electronic records and provide for their secure storage.

Technological Safeguards

- Our computers are programmed to scan for viruses.
- We have rules for the use of faxes and fax equipment is housed in a protected location away from public view.
- We ensure the use of passwords on our computers.

Assessing the Program

OM Financial Inc. regularly assesses their compliance controls every two years. Any weakness in the system is taken into consideration and compliance controls are modified accordingly. Compliance Manuals are updated as per the changes that are required and implemented.

Training

OM Financial Inc. provides training to their front-line and management staff and keep them informed, so they can answer the following questions:

- How do I respond to public inquiries regarding our privacy policies?
- What is consent? When and how is it to be obtained?
- How do I recognize and handle requests for access to PI?
- To whom should I refer complaints about privacy matters?
- What are the ongoing activities and new initiatives relating to our protection of PI?

Clean Desk Policy

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations must be locked when workspace is unoccupied.
3. Passwords should be set for each desktop to avoid unauthorized individual from accessing confidential information.
4. Computer workstations must be shut down completely at the end of the work day
5. Any personal and confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
6. Printed materials must be immediately removed from printers or fax machines.
7. Any documents with restricted/sensitive information no longer being used must be shredded at the end of the day.
8. File cabinets must be kept closed and locked when not in use or when not attended.
9. Keys and passwords must be kept in a safe place.

Canada Anti-Spam Legislation

Our summary below is not exhaustive. Given that these regulations are new and unproven, it is expected that the guidance and industry response with respect to compliance will develop over time.

As of July 1, 2014, all commercial electronic messages (CEMs) that are not exempt must include:

– the name of the sender

– its complete business postal address

– either your phone number, email address or website address

– an "unsubscribe" mechanism, which must take effect within 10 days. The mechanism itself must be valid for 60 days.

Definition of a CEM: any electronic message sent to an electronic address whose purpose is to encourage participation in a commercial activity (e.g. a transaction or commercial transaction) whether or not there is an expectation of profit. According to the CRTC, as of July 1, any electronic request for consent to receive CEMs is in itself a CEM.

Non-CEM communications: Some types of communication are not CEMs, including things like emails between administrative staff and advisors or their clients that relate to ongoing or existing matters.

There are certain exclusions/exemptions. The following list is not exhaustive. (See link for more information: **http://combattrelepourriel.gc.ca/eic/site/030.nsf/fra/00285.html**):

1. Business-to-business activities: CEMs of an employee, representative, advisor or affiliate of an organization with another employee, representative, advisor or affiliate of the organization or other organization that has an existing business relationship with the shipper are exempt and do not require