OM FINANCIAL INC.
A Company With a ♥!

Privacy Breaches

A privacy breach occurs when there is an unauthorized access to, or collection, use or disclosure of PI that contravenes privacy legislation. Typically breaches occur because PI is lost, stolen, disclosed in error or as a consequence of an operational breakdown.

Procedure to Follow for Privacy Breaches:

- **Gather information** about the incident:
  - Date of occurrence
  - Date discovered
  - How discovered
  - Location of the incident
  - Cause of the incident
  - Any other information you can quickly assemble

- **Contain the breach** immediately – don't let any more information escape.
  - Stop the unauthorized practice
  - Recover the records
  - Shut down the system that was breached
  - Revoke or change computer access codes or
  - Correct weaknesses in physical or electronic security.

- **Assess the breach** –The OPCC states that "if the breach appears to involve theft or other criminal activity, notify the police. Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action."

- **If customer information was involved, OM Financial will take the following action;**

  1. **Compliance Officer of OM Financial will notify the insurers involved and**

     Decision regarding who else needs to be apprised of the incident internally and externally. Depending on the nature of the breach, the insurer, OM Financial and Producer should consult on whether affected individuals should be notified, how they will be notified and by whom. The OPCC states "Typically, the organization that has a direct relationship with the customer, client or employee should notify the affected individuals, including when the breach occurs at a third party service provider that has been contracted to maintain or process the personal information." The decision as to whether to notify the affected individuals may have to be delayed in order for a full risk assessment to be conducted.

- **Evaluate the risks** associated with the breach. Find out:

  a. What PI was involved
  b. How sensitive the information is. Generally, the more sensitive the information, the higher risk of harm. Consider these high risk forms of PI:

- Health information
- Government-issued ID such as SINs, driver's licence and health care numbers
- Bank account and credit card numbers
- If a ***combination of PI*** was involved, as this is typically more sensitive. The combination of certain types of sensitive PI along with name, address and DOB suggest a higher risk.

c. How this PI can be used. Can it be used for fraud or other harmful purposes (i.e. identity theft, financial loss, loss of business or employment opportunities, humiliation, damage to reputation or relationships)?

d. Is there a reasonable risk of identity theft or fraud (usually because of the type of information lost, such as an individual's name and address together with government-issued identification numbers or date of birth)?

e. Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?

f. Is there a risk of humiliation or damage to the individual's reputation (e.g. the PI includes mental health, medical or disciplinary records)?

g. Whether the PI was adequately encrypted, made anonymous or otherwise not easily accessible.

h. What is the ability of the individual to avoid or mitigate possible harm?

i. The cause of the breach.

j. The extent of the breach – how many individuals have been affected?

k. Who are they?

l. What harm can result to the Producer and MGA? (Loss of trust, assets, financial exposure, legal proceedings).

Do a thorough post mortem in order to prevent future breaches. What steps are needed to correct the problem? Is this a one-off issue or is it systemic?

Regulatory Audits of PI Management Practices – What To Expect

Section 18 of PIPEDA permits the OPCC to conduct audits if it has "reasonable grounds" to believe that an organization is contravening PIPEDA. OM Financial must receive reasonable notice of an intended audit. Typically, OM Financial would receive a letter from the OPCC notifying us of a complaint or plan to audit, along with the name of the person responsible for the file.

OM Financial reserves the right to contact our own legal counsel and seek direction regarding safeguarding solicitor-client privileged information and whether other parties need to be notified of the investigation or audit.

Note that it is an offence to obstruct an investigation, including concealing information, providing misleading information or refusing to provide information. If it is determined that the complaint or investigation is related to the use of customer information, it is very likely that the insurer(s) whose customer information is involved will need to be notified and kept apprised.

- OM Financial understands that, after receiving the initial information, the person named by the OPCC will communicate in writing or by phone to us

a. How he or she intends to proceed, identifying certain records to review and staff members to interview.

b. Any dates and times for on-site visits, (which can generally be negotiated).

c. We must make every effort to determine the cause and the details and scope of the investigation, including what topics will be covered in staff interviews. This is necessary in order to determine what documentation is required, to allow time to locate and analyze the records and to prepare staff who will be interviewed.

- **<u>During the audit or investigation</u>**:

OM Financial Acknowledges that;

a. The investigator will likely review our privacy procedures and records related to the investigation and meet with designated staff. We will make every effort to ensure that senior officer or Compliance Officer/Privacy Officer can attend any interviews with staff, although the investigator has the right to meet with individuals in private and we must cooperate with these requests.

b. Document all of the details of the investigation, including the auditor's actions, comments and requests along with the material reviewed and the persons interviewed. Gaining more information about the nature of the complaint or alleged non-compliance that gave rise to the investigation is important.

c. While the investigator is entitled to review virtually any record in any format, special care must be taken with any material identified as privileged. We may require legal advice in thisregard.

d. If the investigator requests access to original documents, we must ensure that we retain a copy. (All such documents must be returned to us within 10 days if removed from the premises).

e. If the nature of the complaint or concerns allows for it, we should actively try to resolve the complaint informally and without publicity, seeking an alternative to the OPCC issuing an investigative report.

OM FINANCIAL INC.
A Company With a ♥!

- **Following the audit or investigation:**

a. Before finishing the investigation, the investigator should disclose tentative findings. OM Financial should continue to try to resolve the underlying issues before the investigation is finished.

b. The OPCC is required to provide a report to OM Financial, which contains the findings and any recommendations.

c. It is critically important for OM Financial to consider whether the investigation and resulting findings arose as a result of systemic problems and/or failure to adhere to their policies and procedures. An action plan will be required, along with a timetable for resolution of any issues identified.

OM FINANCIAL INC.
A Company With a ♥!

DATE: November, 2018

SUBJECT: **Privacy – Summary of changes to the Personal Information Protection and Electronic Documents Act (PIPEDA)**

As of November 1, 2018, changes to the **Personal Information Protection and Electronic Documents Act (PIPEDA)** and regulations will come into force. It is important that all distribution partners inform themselves about these new requirements and incorporate them into their privacy policies and procedures.

The main changes that affect those in the life insurance industry are:

- Requirement to notify individuals about security breaches which pose a real risk of significant harm except where prohibited by law
- Requirement to report breaches of security safeguards to the federal Office of the Privacy Commissioner involving personal information that pose a real risk of significant harm[1]
- Requirement to notify other organizations or government institutions that may be able to mitigate that harm
- Requirement to keep records of all privacy breaches for 24 months

What is a security breach?
A security breach is a loss of, the unauthorized access to, or disclosure of, personal information. Breaches can happen when personal information is stolen, lost or mistakenly shared.

What is personal information?
Personal information is information in any form about an identifiable individual.

Significant Harm
Significant harm includes identify theft, financial loss, negative effects to credit score or credit record, loss of employment, loss of business or professional opportunities, damage to reputation or relationships, humiliation, loss or damage to property, and bodily harm.

You are expected to make an assessment to determine if there is a *real risk* of significant harm based on the sensitivity of the personal information involved in the breach and the probability that the information will be misused.

Breach Response
The Privacy Commissioner has identified four key steps in responding to any security breach:

Step 1: Contain the breach
Take immediate steps common sense steps to limit the breach with actions such as stopping the unauthorized practice, recovering records, shutting down the system that was breached, correcting obvious weaknesses in physical security, alerting the privacy officer or others responsible for security in your organization and notifying the police if the breach involves theft or other criminal activity.

---

[1] The provinces of Alberta, British Columbia and Quebec have provincial privacy legislation which has been deemed "substantially similar' to the federal PIPEDA. However, only Alberta has mandatory breach notification requirements. It is not yet clear whether security breaches in those provinces will need to be reported to the federal privacy commissioner.

OM FINANCIAL INC.
A Company With a ♥!

Step 2: Evaluate the risks associated with the breach

Consider whether personal information was involved. Generally, the more sensitive the data, the higher the risk.
Consider what possible uses there are for the personal information. Can it be used for fraudulent or otherwise harmful purposes?
Determine the cause of the breach and whether there is a risk for ongoing or further exposure of the information. Is the information encrypted or otherwise not readily accessible?
Determine what individuals are affected by the breach, how many and what harm may result from the breach.
Determine *real risk of significant harm* based on an assessment of the sensitivity of the personal information involved in the breach and the probability the personal information has been/is/will be misused.

Once you have evaluated the risks, you can determine what other steps you need to immediately take.

Step 3: Notification

Notification of affected individuals and others may be necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed.
If there is a real risk of significant harm, you are required to notify affected individuals, the privacy commissioner, any other government institutions or organizations that could mitigate or reduce the risk of harm (for example, law enforcement) and those to whom you have a contractual obligation (for example, insurance carriers).
Notification should be done as soon as feasible following the breach as time is of the essence. You can file the breach report immediately and further information can be added as it becomes available.
The preferred method of notification is direct to affected individuals by letter, email, phone call or in person. The notification should include the following information:

- Date(s) of the breach or time period over which it occurred
- Description of the breach
- Description of the personal information that is subject of the breach
- Description of the steps taken to reduce the risk of harm that could result from this breach
- Description of the things affected individuals could do to reduce the risk of harm that could result from the breach or to mitigate the harm
- Contact information that the affected individuals can use to obtain further information about the breach.
- That individuals have a right to complain to the Office of the Information and Privacy Commissioner. Provide contact information.

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. As a result of this investigation, you should develop or improve as necessary adequate long term safeguards against further breaches.

Record Keeping

Records must be kept of ALL breaches, even when you have determined there is no risk of significant harm and be kept for a minimum of two years for review by the Privacy Commissioner, if requested.
Records should include, at a minimum:

- Date(s) or estimated date(s) of breach
- Description of the circumstances of the breach
- Nature of the information involved in the breach
- Whether or not the breach was reported to the privacy commissioner or others that were notified
- If not reported, a brief explanation as to why it was determined that there was no risk of significant harm.

Information Resources

Detailed information on all of your privacy obligations can be found at the www.priv.gc.ca. You should also familiarize yourself with the provincial privacy commissioner website if you are licensed in a province where a provincial privacy commissioner is present.

OM FINANCIAL INC.
A Company With a ♥!

Contact Information – Regulator

Office of the Privacy Commissioner of Canada Website: www.priv.gc.ca

This website contains extensive contact information for all provincial privacy regulators and ombudsmen. It is kept up to date and should be our first source of regulatory contact information.

General Inquiries:

Toll-free: **1-800-282-1376**

Phone: **(613) 947-1698**

Fax: **(613) 947-6850**

TTY: **(613) 992-9190** Hours of service are from 8:30 a.m. to 4:30 p.m.

Publication Requests: When requesting publications via e-mail, include your name, telephone number, and return address in order to ensure a reply. Direct your publication request to publications@priv.gc.ca.

To report a breach:

By e-mail: notification@priv.gc.ca;

By phone: 613-995-2042; or,

By mail: Notification Officer

Office of the Privacy Commissioner of Canada
112 Kent Street Place de Ville, Tower B, 3rd
Floor, Ottawa, Ontario, K1A 1H3