# 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 because of an operational breakdown.

**Procedures to follow for Privacy Breaches:**

- **Notify the compliance officer immediately**
- **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 Inc. will take the following actions:***
    - Compliance Officer of OM Financial Inc. will notify the advisors and insurers involved and work with them to determine who needs to be apprised of the incident internally and externally. Seek instructions on how the insurer would like to proceed. The insurer should determine 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 for a full risk assessment to be conducted.

- **Evaluate the risks associated with the breach. Find out:**
  a. What PI was involved?
    - 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 license, 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.

  b. 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)?

c. 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)?

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

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

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

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

h. The cause of the breach.

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

j. Who are they?

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

l. Do we have to report the breach to a regulator?

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

If Advisor or employee information was involved, notify the Compliance Officer immediately. There will likely be no need to notify the insurers, but the Compliance Officer will generally follow the same steps as above with appropriate consideration given to the special sensitivities around employee and Advisor PI.

OM FINANCIAL INC.
*A Company With a ♥!*

# PRIVACY BREACH CHECKLIST

**Step 1: Incident Description**

- When was the date of the incident?
- Who discovered it?
- Details of what happened?

**Step 2: Breach Containment and Preliminary Assessment**

- Have you contained the breach (recovery of information, computer system shut down, locks changed?)
- Have you designated an appropriate individual to lead the initial investigation?
- Have you determined who needs to be made aware of the incident internally and potentially externally at this preliminary stage?
- Does the breach appear to involve theft or other criminal activity? If yes, have the police been notified?

**Step 3: Evaluate the Risks Associated with the Breach**

(i) What personal information was involved?

- What personal information was involved (name, address, SIN, financial, medical)?
- What form was it in (e.g., paper records, electronic database)?
- What physical or technical security measures were in place at the time of the incident (locks, alarm systems, encryption, passwords, etc.)?

(ii) What was the cause and extent of the breach?

- Is there a risk of ongoing breaches or further exposure of the information?
- Can the personal information be used for fraudulent or other purposes?
- Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
- Has the personal information been recovered?
- Is this an isolated incident?

(iii) Who has been affected by the breach (employees, clients, service providers, other organizations)?
(iv) Is there any foreseeable harm from the breach?

- What harm to the individuals could result from the breach (e.g., security risk, identity theft, financial loss, loss of business or employment opportunities, physical harm, humiliation, damage to reputation, etc.)?
- Do you know who has received the information and what is the risk of further access, use or disclosure?
- What harm to the organization could result from the breach (e.g., loss of trust, loss of assets, financial exposure, legal proceedings, etc.)
- What harm could come to the public as a result of notification of the breach (e.g., risk to public health or risk to public safety)?

**Step 4: Notification**

(i) Should affected individuals be notified?

- What are the reasonable expectations of the individuals concerned?
- What is the risk of harm to the individual? Is there a reasonable risk of identity theft or fraud?
- Is there a risk of physical harm? Is there a risk of humiliation or damage to the individual's reputation?
- What are the legal and contractual obligations of the organization?
- If you decide that affected individuals do not need to be notified, note your reasons.

(ii) If affected individuals are to be notified, when and who will notify them?

- What form of notification will you use (e.g., by phone, letter, email or in person, website, media, etc.)?
- Who will notify the affected individuals? Do you need to involve another party?
- If law enforcement authorities are involved, does notification need to be delayed to ensure that the investigation is not compromised?

(iii) What & Who should be included in the notification?
Depending on the circumstances, notifications could include some of the following, but be careful to limit the amount of personal information disclosed in the notification to what is necessary:

- a description of the personal information involved in the breach;
- contact information in your organization who can answer questions or provide further information;
- whether your organization has notified a privacy commissioner's office;
- Should any privacy commissioners' office be informed?
- Should the police or any other parties be informed? This may include insurers; professional or other regulatory bodies; credit card companies, financial institutions or credit reporting agencies; other internal or external parties such as third-party contractors, internal business units not previously advised of the privacy breach

**Step 5: Prevention of Future Breaches**

- What short or long-term steps do you need to take to correct the situation (e.g., staff training, policy review or development, audit)?

OM FINANCIAL INC.
*A Company With a ♥!*

# PRIVACY BREACH TEMPLATE

Date:

| | |
|---|---|
| Name of individual completing the form | |
| Date and location of incident: | |
| Description of incident | |
| Cause of incident | |
| Affected individuals | |
| Personal information involved | |
| Description of action(s) taken to contain breach | |
| Who has been notified and date of notification | |

OM FINANCIAL INC.
*A Company With a ♥!*

# 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 Inc. must receive reasonable notice of an intended audit. Typically, OM Financial Inc. 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 Inc. 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 Inc. understands that, after receiving the initial information, the person named bythe 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 to determine what documentation is required, to allow time to locate and analyze the records and to prepare staff who will be interviewed.

**During the audit or investigation**:

OM Financial Inc. 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 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 this regard.

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.

**Following the audit or investigation:**

**a.** Before finishing the investigation, the investigator should disclose tentative findings. OM Financial Inc. 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 Inc., which contains the findings and any recommendations.

**c.** It is critically important for OM Financial Inc.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. will report applicable privacy breaches to the regulators.

## 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 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

**Office of the Information and Privacy Commissioner of Alberta**: www.oipc.ab.ca

General Inquiries (Edmonton):

Phone: 780-422-6860
Toll-Free: 1-888-878-4044
Fax: 780-422-5682
Email: generalinfo@oipc.ab.ca

(Alberta):

Phone: 403-297-2728
Toll-Free; 1-888-878-4044
Fax: 403-297-2711
Email: generalinfo@oipc.ab.ca

To report a breach:

By email: breachreport@oipc.ab.ca
By mail:
Office of the Information and Privacy Commissioner of Alberta
410, 9925 - 109 Street Edmonton, AB T5K 2J8