Market Surveillance Administrator

Freedom of Information and Protection of Privacy Act

Privacy Breach Report

General Information

A privacy breach occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the *Freedom of Information and Protection of Privacy Act* (*"FOIP" Act)*. The most common privacy breach occurs when personal information is stolen, lost, or accidentally disclosed.

The information that you provide to the MSA is collected under the authority of section 33(c) of *FOIP*. Your personal information is protected by *FOIP* and can be reviewed on request. All collected contact information is maintained with the Market Surveillance Administrator FOIP Coordinator to help respond to requests. Questions regarding the collection, use, or disclosure of this personal information can be directed to the MSA FOIP Coordinator at the contact address below or at foip@albertamsa.ca.

Instructions

Complainants must fill in Part 1 of the Privacy Breach Report, sign the document and send by mail or deliver in person to:

MSA FOIP Coordinator
#500, 400 – 5th Avenue S.W.
Calgary AB T2P 0L6

Phone 403-705-3181 if immediate action is required.

The MSA FOIP Coordinator will contact you on receiving Part 1 and will then complete Part 2. Contact the MSA FOIP Coordinator if additional assistance is required regarding a request. If you are not satisfied with the MSA's response to your request you can contact the Office of the Information and Privacy Commissioner of Alberta to request a formal review.

According to section 65(1) of *FOIP*, a person has a right to request a review by the Information & Privacy Commissioner of Alberta of any decision, act, or failure to act by the public body as it relates to a request.

Additionally, section 65(3) states that a person who believes that the person's own personal information has been collected, used, or disclosed in contravention of Part 2 may ask the Commissioner to review that matter.

A request for a review must be completed in writing and submitted to the Office of the Information & Privacy Commissioner by mail as outlined in section 66(1) of *FOIP*. All requests must be completed within 60 days after the complainant asking for the review has been notified of the decision based on section 66(2)(a)(i) of *FOIP*.

Office of the Information and Privacy Commissioner of Alberta
410, 9925 – 109 Street
Edmonton, Alberta
T5K 2J8
1-888-878-4044
generalinfo@oipc.ab.ca
www.oipc.ab.ca

Review request form can be accessed on the OIPC website.

Privacy Breach Report
Part 1 – Reporting a Breach

Report Date: _____

Complainant Name: _____

Phone Number: _____

Email: _____

Mailing Address: _____

Describe the nature of the breach: _____

_____

_____

_____

_____

Date breach was discovered by Complainant:_____

Date of breach (if known):_____

Personal Information involved (i.e. describe generally SIN Number, Birthdate):

_____

MSA area/staff that has custody/control of records in question:

_____

Action requested: _____

Complainant's Signature:
_____

Date:
_____

Part 2 –Breach Assessment
To be completed by the MSA FOIP Coordinator

A. Risk Evaluation

Date of security evaluation: _____

Department (source of breach): _____

Privacy breach status: ____ Confirmed Privacy Breach

____ Privacy Breach Possible

Describe nature of breach:_____

_____

Estimated number of individuals affected:_____

Type of individual affected: ___ Employee

___ Past Employee

___ Business – Vendor

___ External - Other

Personal information involved (Describe generally i.e. Name, SIN, financial, birth date, employee number):

_____

_____

B. Safeguards

Physical Security

Describe current physical security measures (i.e. locked rooms, locked cabinets, file checkout system):

_____

_____

Technical Security

Describe current technical security measures (i.e. Encryption, Password Access):

_____

_____

Administrative Security

Describe current administrative security measures (i.e. security clearances, policies, training programs):

_____

_____

C. Harm Evaluation

Identify the type of harm(s) that may result from breach:

___ Identity theft
___ Damage to reputation
___ Future breaches due to similar technical failures
___ Risk of physical harm
___ Damage to employment opportunities

D. Notification

Has the Market Surveillance Administrator been notified?

___ Yes Who was notified and when?
_____

___ No When to be notified?
_____

Have affected individuals been notified?

___ Yes Manner of notification:
_____

Why Not?

___ No _____

What information was included in the notification to the complainant?

___ Date of breach

___ Description of the breach

___ Description of the information accessed, collected, used or disclosed

___ Steps taken so far to control or reduce harm

___ Risk(s) to the individual caused by the breach

___ Future steps planned to prevent further privacy breaches

___ Privacy Commissioner contact information

___ Organizational contact information for further assistance

Should the Office of the Information and Privacy Commissioner be notified of the breach?

Factors to consider:

___ The personal information involved is sensitive

___ There is a risk of identity theft or other harm

___ A large number of people affected by the breach

___ The information has not been fully recovered

___ Public body requires assistance in responding to a privacy breach

___ Need to ensure that the steps taken comply with the MSA's obligations under *FOIP*

Comments:_____

_____

_____

E. Prevention

Describe the immediate steps taken to contain and reduce the harm of the breach (i.e. Locks changed, access to files process changed):

_____

_____

_____

Describe the long-term strategies you will take to correct the situation (i.e. Staff training, policy development, privacy and security audit, improved technology architecture, improved physical security):

_____

_____

_____

_____