ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-012

AIR MILES Reward Program

May 11, 2011

(Case File #P1822)

I. Introduction

[1] On April 4, 2011, I received a report from AIR MILES Reward Program ("AIR MILES") of an incident involving the unauthorized access to personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to individuals as a result of the incident, and therefore I require that AIR MILES notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] Under s. 34.1 of the *Personal Information Protection Act* (PIPA), an organization having personal information under its control must, without unreasonable delay, notify me of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), and

(c) to satisfy terms and conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

(i) a corporation,

(ii) an unincorporated association,

(iii) a trade union as defined in the *Labour Relations Code*,

(iv) a partnership as defined in the *Partnership Act*, and

(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] I have jurisdiction in this matter because AIR MILES is an "organization" as defined in section 1(1)(i) of PIPA, and the information at issue in this incident qualifies as "personal information" as defined in section 1(1)(k).

[6] In considering whether to require AIR MILES to notify affected individuals, I am mindful of PIPA's purpose and legislative principles and the relevant circumstances surrounding the reported incident.

III. Background

[7] On April 4, 2011, I received an e-mail report from AIR MILES describing an incident involving the unauthorized access to personal information.

[8] On April 6, 2011, my Office contacted AIR MILES to request that it provide additional information concerning the incident, in order for me to determine whether to require AIR MILES to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a telephone call on April 6, 2011 as well as via fax on May 3, 2011. Via telephone and e-mail between April 8 and May 9, 2011 my Office also discussed the matter with Epsilon Data Management LLC ("Epsilon"), the service provider to AIR MILES where the breach actually occurred.

[9] The circumstances of the incident reported to me are as follows:

- Epsilon is a large, US-based, third-party marketing organization. AIR MILES obtained the services of Epsilon to send email notifications and to manage AIR MILES's rewards program.

- On April 3, 2011, AIR MILES was notified by Epsilon that it had experienced a massive data breach and that AIR MILES Collectors (members who collect AIR MILES points) had been included among the affected individuals.

- Both Epsilon and AIR MILES reported information regarding the nature of the Epsilon data breach including:
    - On March 30, 2011, Epsilon investigated an alert regarding unusual download activity. Epsilon's alert notifications are designed to note any download of a client list.
    - Epsilon determined that login and password credentials for a single Epsilon email application administrator had been compromised.
    - Client lists, consisting of names and email addresses had been downloaded to an FTP site in another country.

- Epsilon reported that at least 50 million email addresses were compromised as a result of the data breach. This number includes not just AIR MILES Collectors, but customers of all of the organizations that were affected by the breach. Epsilon was unable to confirm the exact number of individuals affected because the same email address could have been included in more than one client list, and it is also possible that the same individual could have provided different email addresses to different organizations (e.g. work email, personal email, spam email etc.) Epsilon's contractual obligations prevent it from cross-referencing the information from different clients to determine which information is duplicated.
- Epsilon stated it had strong security measures in place and the data breach was highly sophisticated. It has implemented and maintains an information security program that conforms to the International Organization for Standardization data security standards, notably standards ISO 27001 and ISO 27002.
- Only a small number, approximately 2%, of Epsilon's clients were affected by the data breach.
- Epsilon is working with US law enforcement to investigate the breach and has taken numerous precautions to prevent a future incident.

- AIR MILES provided information regarding the impact of the Epsilon data breach on its Collectors including the following:
  - On April 3, 2011, AIR MILES was notified by Epsilon that its list of e-mailable Collectors may have been compromised.
  - The number of affected AIR MILES collectors in Alberta is 475,000.
  - The personal information downloaded from the Epsilon server from AIR MILES included only:
    - First and last name, and
    - Email address

- On April 4, 2011 AIR MILES sent an email to all of its Collectors notifying them of the breach and the surrounding circumstances. AIR MILES also included additional information instructing clients how to protect themselves online, including email fraud and phishing prevention tips. Information about the breach was also posted on the AIR MILES website and the AIR MILES community page and Facebook page.

- AIR MILES emphasized that it treated the data breach with utmost seriousness and was carefully monitoring the situation and requiring updates from its service provider, Epsilon. Further, although it was not required to do so, AIR MILES also took the proactive step of informing both the B.C. and Federal Privacy Commissioners of the data breach, and did so on April 4, 2011.

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[10] Although it was Epsilon, not AIR MILES that experienced the actual data breach, pursuant to s. 5(2) of PIPA, AIR MILES is responsible for its agent's compliance with the Act. Section 5(2) provides:

> 5(2) For the purposes of this Act, where an organization engages the service of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act.

Therefore, the personal information of the AIR MILES collectors remained within AIR MILES's control.

[11] Pursuant to section 37.1 of PIPA, I have the power to require AIR MILES to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure." In determining whether or not to require AIR MILES to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident. Numerous factors are considered when determining whether a real risk of significant harm has occurred, which include but are in no way limited to: the magnitude of the breach, that is the number of affected individuals, the maliciousness of the breach including whether there are indications personal information was misappropriated for nefarious purposes, the sensitivity of the information and the harm that may result. Each breach must be assessed based on the circumstances of that particular case.

[12] In order for me to require that AIR MILES notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the affected individuals as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[13] In this case, the personal information at issue is of low sensitivity as it includes first and last name as well as email address. AIR MILES confirmed there was no download of any kind of master client list.

[14] AIR MILES noted that the type of harm that could result from the unauthorized access to or disclosure of this information is email phishing, and more particularly, spear phishing. Email phishing is a way for criminals to obtain sensitive personal information, such as usernames, passwords or financial information by masquerading as a trustworthy entity. Spear phishing is a targeted form of phishing where some information is already known about the target and this may improve the chance of success from a phishing attempt. In this case, affected individuals are likely to receive an email from criminals which has the appearance of originating from AIR MILES which could invite the individual to open an attachment with malware or update a "profile" which would provide additional personal information to those with nefarious intentions.

[15] A successful phishing attempt may persuade victims to disclose sensitive personal information that can then be used for theft, fraud, identity theft or other criminal acts, or where a malware install is successful, can do any number of things to an affected computer. All of these possibilities are, in my view, significant harms.

[16] In order for me to require AIR MILES to notify its affected Collectors, however, there must also be a "real risk" of significant harm to the Collector as a result of the incident. This standard does not require that harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. Further, there must be a cause and effect relationship between the incident and the possible harm.

[17] As part of its dialogue with this Office, AIR MILES presented the viewpoint that there was no "real risk" of significant harm to its Collectors as a result of the Epsilon breach. It stated that by itself, the information disclosed is insufficient to access Collector personal information of Collector accounts. AIR MILES pointed out that it had quickly notified its Collectors who had been affected by the breach and provided them with information about how they could further protect themselves.

[18] However, whether or not an organization has already notified affected individuals is not a factor for consideration in determining whether there is a real risk of significant harm. Prior notification, assuming it is done in accordance with s. 19 of the PIPA Regulation, may relieve an organization of a requirement to notify again, but it does not affect whether the breach incident itself is considered a real risk of significant harm to affected individuals. This office has already published numerous decisions where the fact that an organization had already notified affected individuals had no bearing on whether there was a real risk of significant harm.

[19] In deciding whether there exists a "real risk" of harm in this case, I considered that 475,000 AIR MILES Collectors in Alberta were affected by the Epsilon breach. I also carefully considered AIR MILES's argument that a "real risk" of significant harm would include more personal information than just first and last name and e-mail address.

[20] In my opinion, there is a clear cause and effect relationship between the potential harm that may arise from the Epsilon breach. Affected individuals are likely to be targeted with "spear phishing" emails which directly target them as known Collectors of AIR MILES. It is to be hoped that most individuals will ignore these emails, particularly so in cases where they have received notification of the breach and potential risks. However, a small (it is hoped) portion of affected individuals are likely to either open attachments with malware or be tricked into providing additional information. This is the known pattern that is used by criminals when attempting to obtain personal information. Phishing attempts have been successful in the past and there is no evidence to indicate that the information obtained through the Epsilon breach will be treated any differently.

[21] In this case, two factors in particular are relevant to my assessment of whether a "real risk" exists. These are 1) the magnitude of the Epsilon breach and the number of

affected AIR MILES Collectors and 2) the sophistication of the attack and the belief that Epsilon was targeted for nefarious purposes. The Epsilon breach was not an accidental loss or disclosure of personal information; it was a targeted attack to obtain personal information. This is a critical fact in my evaluation of the real risk in this situation. It is a well-known fact that identity theft and fraud are a booming business for organized crime and in the circumstances of this case, it is reasonable to assume that Epsilon was targeted for nefarious purposes.

[22] Nearly half a million Albertan AIR MILES Collectors were affected by the Epsilon breach and the evidence at this point clearly indicates that the information was accessed and downloaded for nefarious purposes. There is no way to predict with certainty what will happen as a result of the Epsilon breach; however, it is not mere speculation, but a reasonable assumption that at some point in the future, the affected AIR MILES Collectors will be targeted by spear phishing emails as a result of the Epsilon breach. To put it into perspective, even if there is only a one in a million chance that an AIR MILES Collector will be misled by a spear phishing email, either by providing personal information or intentionally or accidentally clicking an attachment that will install malware, with those rare odds, at least two affected individuals in Canada would actually be affected as a result of the breach.

[23] Given the information reported by both AIR MILES and Epsilon, I have decided that there is a real risk of significant harm to individuals as a result of this incident. Although the information at issue is of low sensitivity, I have based my decision on the following factors: the personal information was almost certainly taken for nefarious purposes and the large magnitude of the breach makes it likely that some spear phishing attempts will be successful. Where a spear phishing attempt is successful, significant harms such as fraud and identity theft are likely to result.

V. Decision

[24] I understand AIR MILES has already notified all of the affected individuals by way of an email sent on April 4, 2011. I further note that AIR MILES's notification was compliant with section 19.1 of the PIPA Regulation and therefore I will not require AIR MILES to notify affected individuals again.

[25] The Epsilon data breach received a great deal of media attention. AIR MILES was one of the few organizations that took immediate steps to notify affected individuals and proactively take steps to mitigate any harm that may result. I commend AIR MILES for its rapid response to the breach and its cooperation with and helpful submissions to this office. Although a breach cannot always be prevented, an organization can certainly mitigate risks through responding to the situation and notifying affected individuals.

Frank Work, Q.C.
Information and Privacy Commissioner