ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-034

Delta Hotels and Resorts

September 20, 2011

(Case File #P1958)

I. Introduction

[1] On August 17, 2011, I received a report from Delta Hotels and Resorts (Delta) of an incident involving 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 Delta 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 Delta 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 Delta 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 August 17, 2011, I received a written report from Delta describing an incident involving unauthorized access to personal information.

[8] On August 25, 2011, my Office contacted Delta to request that it provide additional information concerning the incident, in order for me to determine whether to require Delta to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls between August 25, 2011 and September 12, 2011.

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

- On July 11, 2011, Delta was contacted by an "ethical hacker" and advised he or she had accessed a web-facing server containing information on its legacy loyalty program.
- Delta confirmed that a web-server hosting 18 databases had been accessed by an unauthorized individual sometime between June 28, 2011 and July 11, 2011.
- The information on the server relates to a variety of sales, loyalty and marketing programs offered by Delta.
- Three of the databases contain personal information.
    - The largest database contains the personal information of individuals who participated in Delta's loyalty program between 2001 and 2006. The personal information in this database that was subject to unauthorized access consists primarily of name, address, telephone number, frequent flyer number, email address and credit card number and expiry dates.

    - The remaining two databases contain personal information of less than 100 individuals each who had received food or beverage rewards or a corporate gift. These records did not contain credit card information.
- Delta conducted an internal assessment that indicated that the personal information of 92 individuals contained credit card information that had not yet expired.
- Delta retained the services of a security firm to conduct a more detailed analysis of the records. It established that 145 589 records were affected by the incident. Of these records, 118 091 contained an expired credit card number and 2 314 contained active credit card numbers (i.e. where the expiry date on the credit card had not yet passed).
- On August 26, 2011, Delta wrote to the 2 314 individuals where unauthorized access to unexpired credit card number had taken place and notified them of the incident.

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

[10] Pursuant to section 37.1 of PIPA, I have the power to require Delta 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 Delta to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

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

[12] Delta assessed the risks associated with this incident and voluntarily notified the 2 314 individuals where the hacker had accessed an unexpired credit card number on August 26, 2011 on the basis that these individuals were at risk of identity theft. Delta did not notify the other individuals as it believed that the risk of harm to these individuals was low given that any credit card number on file had expired.

[13] I agree with Delta's assessment that those individuals where the hacker accessed an unexpired credit card are facing a real risk of significant harm. The data elements accessed place these individuals at an increased risk of identity theft or some form of credit card fraud.

[14] That being said, I disagree with Delta's assessment that the individual where expired credit card information was accessed are not facing a real risk of significant harm. Many financial or credit granting institutions will allow a customer to maintain a credit card number over several renewal cycles. In these cases, when a credit card nears expiry, the institution will mail the customer a new card with the same credit card number but a new expiry date. Furthermore, credit cards are renewed on a predictable and

established cycle. In my opinion, it would not be difficult for an individual who wished to engage in identity theft to derive the new expiry date where they had access to a valid credit card number and a previous expiry date. While this may require some effort on the part of an individual who wished to do harm, it is not inconceivable that they could take the steps necessary to establish the new credit card expiry date. The risk facing an individual in these circumstances is as real and the potential harm is as significant as it is to those individuals where the unauthorized access included an unexpired credit card number.

[15] I have decided that there is a real risk of significant harm to all of the individuals where credit card information was accessed as a result of this incident, not just those where the information accessed included an unexpired credit card number. I have based this decision on the nature of the personal information that was subject to unauthorized access and the ease with which this information could be used for identity theft or other credit card fraud.

V. Decision

[16] Based on the information reported to me by Delta, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require Delta to notify affected individuals. I understand Delta has already notified those individuals where the unauthorized access included an unexpired credit card number in accordance with section 19.1 of the *Personal Information Protection Act Regulation*. I do not require Delta to notify these individuals again, but do require it to notify the 118 091 individuals whose expired credit card information was accessed and who did not receive previous notification. This notification must be in accordance with section 19.1 of the *Personal Information Protection Act Regulation*. Delta must also confirm in writing to my Office that it has done so on or before October 14, 2011.

Frank Work, Q.C.
Information and Privacy Commissioner