ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-020

HONDA CANADA INC. and HONDA CANADA FINANCE INC.

July 13, 2011

(Case File #P1874)

I. Introduction

[1] On May 11, 2011, I received a report from Honda Canada Inc. and Honda Canada Finance Inc. (collectively "Honda") 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 Honda 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 Honda 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 Honda 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 May 11, 2011, I received a written report from Honda describing an incident involving the unauthorized access to personal information.

[8] On May 18, 2011, my Office contacted Honda to request that it provide additional information concerning the incident, in order for me to determine whether to require Honda to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and email correspondence between May 19 and June 21, 2011.

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

- In 2009, Honda sent letters inviting its customers to register in a "My Honda/My Acura" web portal which would allow customers online access to various vehicle information such as: warranty, maintenance, campaign information, extended warranty account information and the latest Honda product news and event information.

- Honda's invitation letters to its customers included a Personalized URL, a "PURL" for customers to copy and paste into their web browser which would allow them to expedite the registration process.

    - The PURL registration pre-filled the customer's information with the following: last name, postal code and vehicle identification number on the first page. The second page pre-filled the customer's name, address and vehicle identification number.

    - For approximately half of the individuals who had a PURL, additional information was pre-populated on another part of the website. This additional pre-populated information included: telephone number and email address.

- On March 2, 2011, Honda reviewed its February activity reports and found there had been an unusual volume of requests from a single IP address (the "Anomaly IP") between February 12 – 23, 2011. Honda initially believed there had been a reporting error, but upon further investigation, it discovered 26,632 PURLS had been accessed. (Honda had created a total of 283,321 PURLS.)

- In order to pass beyond the second page of the web portal to complete registration, an email address and password had to be entered. Upon further review, Honda confirmed that no attempts were made by the Anomaly IP to enter information. Honda further determined that no attempts were made by the Anomaly IP to access the "MyFinance" portion of the PURLS.

- Honda determined the personal information of 26,632 individuals was accessed during the breach. Of these individuals, one person was from Alberta and the remainder were from Ontario. This personal information consisted of the following:
    - Name,
    - Address, and
    - Vehicle Identification Number[1]

- For approximately half of these 26,632 affected individuals (including the one Albertan) two additional data elements were populated on another portion of the accessed website. This additional personal information included:
    - Telephone number; and
    - Email address.

- Honda was unable to determine exactly how the breach occurred. As a result, there remains a possibility that its database could have been accessed; however Honda cannot confirm whether the database was accessed. If the database was accessed, it is possible that the same information (name, address and vehicle identification number) for the full 283,321 customers was accessed. Of these, 21,667 were Albertans.

- Honda further stated that if the database was accessed during the breach, it is possible that the Honda Canada Finance Inc. account numbers for 36,833 individuals were accessed. These are all of the individuals who had financing through Honda. Honda was able to confirm that the *only* information that could have been accessed was the account number, not the amount of financing, or

[1] There is some issue as to whether a vehicle identification number should be considered "personal information" under s. 1(1)(k) of PIPA for organizations subject to this Act. In the Alberta Court of Appeal's decision, in *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)* 2011 ABCA 94 [Leon's], the majority held at paragraph 49 that a license plate could not be considered personal information because it is "about" the vehicle. An obiter comment in the same paragraph (49) further elaborated that vehicle information such as serial numbers or VINs, as well as street addresses would not be considered personal information. An application for leave to appeal the Leon's Decision is currently pending before the Supreme Court of Canada.

payment amounts or any other information regarding financing. Honda also stated that because there is a possibility that finance account numbers could be at risk, it has put additional protections in regarding interactions with customer service representatives so that the finance account number alone, or in combination with other personal information accessed during the breach cannot be used to obtain additional information.

- Honda conducted an internal investigation of the breach. Honda's Privacy Officer was not notified about the breach until April 14, 2011. The Toronto Police and the Canadian Anti-Fraud Centre were notified of the breach on May 10, 2011. This office was notified the next day, on May 11, 2011.

- Upon its review of the breach, Honda concluded that its internal delay in reporting the incident to the Privacy Officer was a result of the customer service team and information services team attempting to discover the cause of the breach. Honda indicates its teams will be instructed on the need to escalate privacy breaches in a timely fashion, even if the matter is still under investigation.

- As a result of the breach, Honda implemented numerous steps to improve its security including:
    - Blocking the Anomaly IP address;
    - Disabling PURL registration, therefore, even if another breach is attempted from a different IP address, the culprit will be unsuccessful;
    - Increasing due diligence of data exchange protocols;
    - Conducting enhanced due diligence on security measures
    - Reviewing its internal processes regarding the security of customer data;
    - Enhancing its internal rules and processes to promote timely escalation of incidents after discovery; and
    - More frequent monitoring and reporting of traffic to "MyHonda" and "MyAcura" webpages.

- Honda mailed notification letters to all 283,321 individuals who *may* have been affected by the breach, not just the 26,632 individuals who were affected.

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 Honda 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 Honda 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 Honda notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to those 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.

[12] In this case, the personal information at issue is of low sensitivity as it consists of names, addresses, vehicle identification numbers[2], telephone numbers, and email addresses.

[13] I did not find it necessary to consider the VIN as personal information in arriving at my decision in this matter.

[14] Honda noted the kind of harm that could arise from the breach may include targeted mailings, where affected individuals are urged to contact Honda (a false representative) and perhaps provide additional personal information or money for a service that won't occur. Similarly, because email addresses may be at risk for some of the affected individuals, there is a risk of spear-phishing. In a spear phishing attack, affected individuals may receive an email from "Honda" (again a false representative) which directs the individual to open an attachment with malware or directs the individual to another website etc. where additional personal information may be gathered. Where a phishing attempt is successful, it can lead to fraud or identity theft which are, in my view, significant harms.

[15] In order for me to require Honda to notify affected individuals, however, there must also be a "real risk" of significant harm to the employee as a result of the incident. This standard does not require that significant 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.

[16] In deciding whether there exists a "real risk" of harm in this case, I considered that Honda was targeted over a period of time by a single IP address which had accessed over 26,000 PURLs over an approximate 2 week period in February 2011. This type of targeted behaviour is a strong indication that the personal information available through Honda's website would be used for nefarious or malicious purposes such as fraud and identity theft.

[17] Given the information reported by Honda, I have decided that there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the following factors: the type of information involved could be used to commit fraud and identity theft, which is a significant harm and the targeted nature of the access indicates a malicious intent, and therefore creates a real risk.

V. Decision

[18] Based on the information reported to me by Honda, I have concluded there is a real risk of significant harm to individuals as a result of this incident. I require Honda to

[2] *Ibid.*

notify affected individuals. I understand Honda has already notified all of the affected individuals via mailings sent out after May 13, 2011. I further note that Honda's notification was compliant with section 19.1 of the *Personal Information Protection Act Regulation*, and therefore I will not require Honda to notify affected individuals again.

Frank Work, Q.C.
Information and Privacy Commissioner