ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-021

T&T SUPERMARKET INC.

July 11, 2011

(Case File #P1922)

I. Introduction

[1] On June 24, 2011, I received a report from T&T Supermarket Inc., ("T&T" or the "Organization") of an incident involving the loss of and 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 T&T 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 T&T 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 T&T 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 June 24, 2011, I received a written report from T&T describing an incident involving the loss of and unauthorized access to personal information.

[8] On June 27, 2011, my Office contacted T&T to discuss details regarding the incident, and obtain further clarification on some points in order for me to determine whether to require T&T to notify individuals under subsection 37.1(1) of PIPA. The unauthorized access to personal information of T&T customers and vendors occurred on June 6, 7, 11 and 14 through 17, 2011.

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

- On June 14, 2011, the Information Technology department determined there had been unauthorized access through the T&T website to databases (on a server located in Vancouver, B.C.) containing customer, job applicant, and vendor personal information.
- A review of database contents showed that a very high number of fields were modified, and that the modified information contained a redirect link to an external web page.
- The unauthorized access to customer and job applicant data occurred on June 6, 11 and 14, 2011. Access to the vendor database occurred on June 14, 2011.
- On June 6, 11 and 14-17, 2011, multiple files were written to the system to redirect users to an external page that possibly contained malware. As a result of the malware files, visitors to the site on June 6, 7 or 11, 2011 may have been redirected—without their knowledge—to a non-T&T website. This website may have displayed a message directing users to start a scan by clicking a button on the screen which activated the download of additional software from visitors' computers in an attempt to gather personal information. A similar redirection occurred of T&T vendors.
- On June 14, 2011, the T&T website was shut down and the corrupted data tables were restored and security of the site was strengthened before the site was brought

back up. On June 17, 2011, T&T applied the same solution to its vendor database.

- The types of individuals affected by the breach were customers who registered to receive e-flyers or placed an order online for pickup at a store; job applicants; and vendors.
- The personal information at issue as a result of the breach is contained in the table below:

Customer Personal Information	
User name	Cell phone number
Password	Fax
First and last name	Age
Email	Gender
Home address	Province, city, postal code
	Phone number
Job Applicants' Personal Information	
Legal first and last name	University Name
Chinese name	Year of completion
Address	Major
Province, city, postal code	Attending institution
Phone number	Disability status
Cell phone number	Criminal Offence (detail if any)
E-mail	Legal to work (yes or no)
Gender	Highest level of education
Current and previous positions held	Valid driver's license (yes or no)
Current and previous employers name	Family member in T&T
Current and previous salary	
Vendor Personal Information	
English and Chinese name	User ID
Alternative name	Username and password

- The total number of individuals affected in Alberta (and Canada) are as follows:
    - Customers: 4602 (47 988)
    - Job applicants: 591 (8948)
    - Vendors: 14 (382)
- Measures taken by T&T following the breach include a shut down and an assessment of its web application architecture and associate hardware/software infrastructure for any additional security vulnerabilities.

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

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

[10] In order for me to require that T&T notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to those customers, job applicants, and vendors as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects. 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.

[11] In this case, the personal information at issue is of moderate to high sensitivity as it includes, among other data elements, such things as name, address, phone numbers, gender, disability status, and details on criminal history of job applicants.

[12] This information is information that could be used to cause significant harm to individuals. T&T noted that the type of harm that could result from the unauthorized access this information is e-mail 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 T&T 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. In effect, T&T found during its investigation into the breach that T&T customers, job applicants, and vendors were redirected from T&T's website to another website.

[13] In order for me to require T&T to notify its customers, job applicants, and vendors, however, there must also be a "real risk" of significant harm to the individuals 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.

[14] In deciding whether there exists a "real risk" of significant harm in this case, I considered that the information at issue is of moderate to high sensitivity; that T&T had discovered that the hackers had been successful at modifying data fields and redirecting visitors to the website to an alternate site; that phishing attempts were likely; and that T&T believes the breach was done with malicious intent.

[15] Given the information reported by T&T, I have decided that there is a real risk of significant harm to individuals as a result of this incident.

V. Decision

[16] I understand T&T has already notified all of the affected individuals by way of letters sent via e-mail (in English, French, and Chinese) on June 28, 2011. T&T also offered to provide customer support via e-mail and telephone, and issued a press release to alert the public as to the compromise of T&T's site. I require T&T to notify affected individuals. I further note that T&T's notification was compliant with section 19.1 of the PIPA Regulation, and therefore, I will not require T&T to notify affected individuals again.

Frank Work, Q.C.
Information and Privacy Commissioner