



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	W.W. Grainger Inc. (Organization)
Decision number (file number)	P2018-ND-032 (File #006611)
Date notice received by OIPC	September 19, 2017
Date Organization last provided information	October 27, 2017
Date of decision	February 28, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• home address,• social insurance number, and• retirement benefits information. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p> <p>The information was collected from Albertans via the Organization’s website.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On August 23, 2017, a laptop was stolen from a vehicle belonging to an employee of the Organization.• The same day, the incident was reported to the police and to the Organization.

	<ul style="list-style-type: none"> • The laptop was password protected and had remote wipe capability. • On August 24 and 25, 2017, the Organization analyzed the files on the computer using system backups and identified the personal employee information on the laptop.
Affected individuals	The incident affected 9,317 Canadians, including 3,244 Alberta residents.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Disabled the employee’s network and all other IT credentials. • Laptop is set to automatically wipe the contents the next time it connects to the internet. • Working closely with law enforcement and outside security experts. • Provided twelve (12) months of complimentary identity protection and twelve (12) months of complimentary credit monitoring.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on September 18, 2017 and October 31, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be “significant.” It must be important, meaningful, and with non-trivial consequences or effects.</p>	<p>The Organization did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated “While we have no indication that any personal information has been access by an unauthorized person or used inappropriately, as an added precaution, [we are] providing [affected individuals] with 12 months of complimentary identity protection and 12 months of complimentary credit monitoring.”</p> <p>In my view, the contact and identity information, along with the financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.</p>
<p>Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.</p>	<p>The Organization did not specifically provide an assessment of the likelihood that significant harm would result from this incident.</p> <p>In my view, the likelihood of harm resulting from this incident is increased as the breach was a result of malicious intent (vehicle break-in and theft). The laptop was not encrypted and has not been recovered.</p>
DECISION UNDER SECTION 37.1(1) OF PIPA	
Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.	

The contact and identity information, along with the financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased as the breach was a result of malicious intent (vehicle break-in and theft). The laptop was not encrypted and has not been recovered.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by letter on September 18, 2017 and on October 31, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner