



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	WP Technology Inc. (Organization)
Decision number (file number)	P2017-ND-71 (File #001361)
Date notice received by OIPC	August 11, 2015
Date Organization last provided information	May 9, 2017
Date of decision	June 7, 2017
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’s head office is in Toronto, Ontario. It is an “organization” as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved some or all of the following information:</p> <ul style="list-style-type: none">• name,• city and country,• email address,• one way encrypted (hashed) password,• gender,• telephone number,• date of birth,• last login IP,• Tumblr credentials (usernames and passwords),• profile links to third party platforms like Facebook, Twitter and Smashwords. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected from residents of Alberta via the Organization’s website wattpad.com.</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 May 29, 2015, the Organization identified an unauthorized user in its computer system. • Information in the Organization’s user database includes the user’s public profile that is publicly displayed on the Organization’s platform and non-profile information that is used for internal purposes. • The attack was identified and terminated while the Organization was investigating the incident. • The Organization determined that only a partial file containing user records may have been transmitted outside of the Organization’s systems.
Affected individuals	The incident affected 36,000 Alberta residents.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Blocked the unauthorized access within hours of identification and initiated an investigation. • Affected individuals were advised to change their Wattpad and Tumblr passwords, and passwords on other accounts where the same password was used. • Affected individuals were advised to guard against phishing scams.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on May 29, 2015.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
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>The Organization reported that “In our view, the most likely harm is phishing. We do not think this is a significant harm since it is a general internet risk that people are aware of and on guard against.”</p> <p>In my view, the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses and credentials could also be used for phishing purposes. These are significant harms.</p>

<p>Real Risk</p> <p>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 reported that “We believe the overall likelihood of significant harm to be low. The attack was identified and terminated while in progress. In our investigation, we determined that only a partial file containing user records may have been transmitted outside our systems. The attacker was not fully successful in obtaining what they wanted. The information contained in our user database is not highly sensitive.”</p> <p>In my view, the likelihood of harm resulting from this breach is increased because the incident was the result of malicious intent (deliberate intrusion). Although the Organization believes only a partial file was successfully transmitted outside its systems, this cannot be known for sure and much of the information at issue can be used to cause significant harm. The information has not been recovered.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<p>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.</p> <p>The contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses and credentials could also be used for phishing purposes. These are significant harms. The likelihood of harm resulting from this breach is increased because the incident was the result of malicious intent (deliberate intrusion). Although the Organization believes only a partial file was successfully transmitted outside its systems, this cannot be known for sure and much of the information at issue can be used to cause significant harm. The information has not been recovered.</p> <p>I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization notified affected individuals by email on May 29, 2015 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner