



**PERSONAL INFORMATION PROTECTION ACT**  
**Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	Guess?, Inc. (Organization)
<b>Decision number (file number)</b>	P2022-ND-005 (File #022143)
<b>Date notice received by OIPC</b>	July 9, 2021
<b>Date Organization last provided information</b>	July 9, 2021
<b>Date of decision</b>	March 7, 2022
<b>Summary of decision</b>	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose personal information was collected in Alberta, pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA “organization”</b>	The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
<b>Section 1(1)(k) of PIPA “personal information”</b>	<p>The incident involved all or some of the following information about applicants for employment and current or former employees:</p> <ul style="list-style-type: none"><li>• name,</li><li>• social Insurance numbers,</li><li>• driver's license numbers,</li><li>• passport numbers, and/or</li><li>• financial account numbers.</li></ul> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.</p>
<b>DESCRIPTION OF INCIDENT</b>	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
<b>Description of incident</b>	<ul style="list-style-type: none"><li>• The Organization recently completed an investigation regarding a cybersecurity incident designed to encrypt files and disrupt business operations.</li></ul>

	<ul style="list-style-type: none"> <li>• The Organization’s investigation determined that there was unauthorized access to certain of its systems between February 2, 2021 and February 23, 2021.</li> <li>• On May 26, 2021, the investigation determined that personal information related to certain individuals might have been accessed or acquired by an unauthorized actor.</li> <li>• The Organization said additional work was required to identify addresses for involved individuals. This work was completed on June 3, 2021.</li> </ul>
<b>Affected individuals</b>	The incident affected 1304 Canadians, including 7 individuals whose personal information was collected in Alberta.
<b>Steps taken to reduce risk of harm to individuals</b>	<ul style="list-style-type: none"> <li>• Conducted an investigation.</li> <li>• Notified law enforcement.</li> <li>• Implemented additional security protocols such as a new training strategy for all employees, multi-factor authentication and endpoint solutions on all servers.</li> <li>• Offered complimentary credit/identity monitoring to all involved individuals.</li> </ul>
<b>Steps taken to notify individuals of the incident</b>	Affected individuals were notified by letter on July 9, 2021.
<b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b>	
<b>Harm</b> 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.	The Organization reported,  <i>Guess considers that the goal of the threat actor was to encrypt and steal data in an attempt to extract a ransom payment from Guess and not to perpetrate any fraud against individuals. Therefore, the consequence of the breach are most likely to be limited to loss of control of personal data. However, it is also possible that the personal data will be disseminated beyond the threat actor or published online.</i>  In my view, a reasonable person would consider the identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss.
<b>Real Risk</b> 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.	The Organization reported,  <i>While Guess' business and information to use for leverage to obtain ransom was the most likely target of the incident, there is some risk that the individual information involved will be disseminated or missused [sic]. Guess has not received any reports that the information has been missused [sic].</i>

	<p>In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand). The lack of evidence that the personal information has been misused is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Although the Organization reported that “<i>While Guess' business and information to use for leverage to obtain ransom was the most likely target of the incident,</i>” this is speculation as to the motives of the unauthorized third party. Further, the information may have been available to the unauthorized third party for approximately 20 days.</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.

A reasonable person would consider the identity and 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 because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand). The lack of evidence that the personal information has been misused is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Although the Organization reported that “*While Guess' business and information to use for leverage to obtain ransom was the most likely target of the incident,*” this is speculation as to the motives of the unauthorized third party. Further, the information may have been available to the unauthorized third party for approximately 20 days.

I require the Organization to notify the affected individuals whose personal information was collected 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 July 9, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack  
Assistant Commissioner, Operations and Compliance