



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Western Union Financial Services Inc. (Organization)
Decision number (file number)	P2017-ND-156 (File #007035)
Date notice received by OIPC	November 8, 2017
Date Organization last provided information	November 8, 2017
Date of decision	November 27, 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 operates across Canada, including in Alberta, and is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The information at issue includes some or all of the following for affected individuals:</p> <ul style="list-style-type: none">• name,• address,• contact information,• identity information (driver’s license numbers and other government-issued identification numbers and passport numbers),• transaction data (including bank account details), and• basic human resources information. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</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">• Until July 2016, the Organization used a third-party vendor’s external system for secure storage services.

	<ul style="list-style-type: none"> • In late July 2016, the Organization noticed suspicious activity in the system and commenced an investigation. • The investigation found that a “malicious computer intrusion had been mounted against the vendor’s system, involving exposure of data that had been placed in files in the storage solution...” and “A small percentage of these files contained personal data.” • The Organization reported it believes the intrusion took place during the month of July 2016.
Affected individuals	The Organization reported it will be notifying 17,668 Canadians, including 3,304 residents of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Immediately ceased using the storage solution and vendor. • Notified law enforcement. • Retained external forensic experts to analyze the data that might have been exposed or exfiltrated.
Steps taken to notify individuals of the incident	The Organization reported it “intends issuing notifications ... on November 9, 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 the type(s) of harm that might result from this incident but reported that it is not aware of any “incidences of fraud, identity theft or other harm to any individual data subject associated with the incident” but that it intends to provide affected individuals with “free identity monitoring services”.</p> <p>In my view, the identity, financial and employment (human resources) information at issue could be used to cause the harms of identity theft, fraud and financial loss. These are significant harms.</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 reported that it is “of the view that the overall risk that there will be any misuse of any of the personal data in the files is slight given the highly unstructured and inaccessible nature of the data and manner in which it was stored, given the complexity involved in analysing the personal and non-personal data such that any personal data would be identified and made usable (as demonstrated by the complexity of the analysis which [the Organization] has had to undertake), and given the expertise and resources needed to assess the data and generally to render it intelligible and usable. Nor is [the Organization] aware of any incidences of fraud, identity theft or other harm to any individual data subject associated with the incident.”</p>

	<p>In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion) and the information may have been exfiltrated and exposed since July 2016. Although it has been complex and time-consuming for the Organization to review and assess the data involved in this incident, I note that the individual(s) responsible for the intrusion do not have to make <i>all</i> the information intelligible and usable in order to use it to cause harm to affected individuals.</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 identity, financial and employment (human resources) information at issue could be used to cause the harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized intrusion) and the information may have been exfiltrated and exposed since July 2016. Although it has been complex and time-consuming for the Organization to review and assess the data involved in this incident, I note that the individual(s) responsible for the intrusion do not have to make *all* the information intelligible and usable in order to use it to cause harm to affected individuals.

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).

In its report of the incident, the Organization said that it would notify affected individuals beginning November 9, 2017. I require the Organization to confirm to my office within 10 days of this decision that it has notified affected individuals in Alberta in accordance with the Regulation.

Jill Clayton
Information and Privacy Commissioner