Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	ULS Maintenance & Landscaping Inc. and Urban Life Solutions Inc. (Organization)
Decision number (file number)	P2021-ND-336 (File #021676)
Date notice received by OIPC	May 14, 2021
Date Organization last provided information	December 16, 2021
Date of decision	March 10, 2022
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 whose personal information was collected in Alberta pursuant to section 37.1 of *the Personal Information Protection Act* (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"	The incident involved all or some of the following information: • name, • telephone number, • pay amount, • deductions from pay, • redacted social insurance numbers, and • banking information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization uses a third party service provider, Dayforce. • On or about May 27, 2021, a human resources employee was speaking to a former employee who, prior to their termination, worked in payroll administration for the Organization. During that conversation, the former employee made remarks suggesting they had (unauthorized) access to the Organization's payroll information. • The matter was escalated for investigation. In conjunction with Dayforce, the Organization determined "that a Super Admin role had been established within … payroll systems prior to the former employee's departure, in a covert manner such that it was not easily detectable." • The Organization confirmed that records were downloaded by the former employee. The Organization believes the downloaded records were destroyed by the former employee; however, it had not received confirmation of destruction. • Unauthorized access was possible between March 22, 2021 and May 28, 2021.
Affected individuals	The incident affected 265 individuals, including 217 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Retained professional advice and investigated the incident. • Conducted a review of IT systems. • Deleted or changed passwords of potentially affected user accounts. • Provided affected individuals with credit monitoring services. • Reviewed and augmented multi-factor authentication and security protocols already in place. • Reported the incident to police.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on June 11, 2021.
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.	The Organization reported that "Possible harms include: identity theft and financial fraud." I agree with the Organization's assessment. A reasonable person would consider the contact, identity, financial, and employment information at issue could be used to cause the harms of identity theft and fraud. Employment information (pay and pay deductions) could also be used to cause embarrassment, or loss of employment, business or professional opportunities. These are all significant harms.

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.	The Organization reported: *Given that the majority of the information that could otherwise have been used to engage in identity theft and fraud was obscured in the reports downloaded, [the Organization] assesses the risk of significant harm as low.* On December 16, 2021, the Organization submitted an update which included a characterization of the former employee's unauthorized access and use of the personal information at issue. The Organization also said: *We believe that the records were destroyed, but are awaiting confirmation from [the former employee].* 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 action of an individual who deliberately, and covertly, created and used a "Super Admin" account to access, download, and use personal information without authorization. Further, unauthorized access was possible for approximately 2 months and the Organization has not been able to confirm the destruction of copies created by the unauthorized individual.

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 contact, identity, financial, and employment information at issue could be used to cause the harms of identity theft and fraud. Employment information (pay and pay deductions) could also be used to cause embarrassment, or loss of employment, business or professional opportunities. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the action of an individual who deliberately, and covertly, created and used a "Super Admin" account to access, download, and use personal information without authorization. Further, unauthorized access was possible for approximately 2 months and the Organization has not been able to confirm the destruction of copies created by the unauthorized individual.

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 email on June 11, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner