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	Pleasant Solutions Inc. (Organization)
Decision number (file number)	P2018-ND-169 (File #007888)
Date notice received by OIPC	February 23, 2018
Date Organization last provided information	March 9, 2018
Date of decision	December 14, 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 *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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • personal email address, • mailing address, • date of birth, • emergency contact information, • Social Insurance Number, • direct deposit information (void cheques), • driver's license photo, • passport number, • RCMP background check, • diploma, • Alberta Health Care Number, • university transcript, and • permanent residency card. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 6, 2017, the Organization's CEO found a USB keylogger on his computer. The Organization reported the matter to law enforcement, and commenced an investigation. • On October 6, 2017, an employee with the Organization was arrested, his equipment was seized and cloud data copied. • The investigation found that the employee accessed the CEO's computer remotely on September 25, 2017 using a password obtained with the keylogger. Employee files were copied from the CEO's computer.
Affected individuals	The incident affected 134 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to law enforcement and cooperated with investigations. • Seized the employee's equipment, including hard drive with employee files. • Will forward any suspicious activity reports by an affected individual to the local police service for investigation. • Provided 1 year of credit monitoring to affected individuals.
Steps taken to notify individuals of the incident	The Organization notified current employees during a staff meeting on December 6, 2017. The Organization reported that the police advised the Organization that the police "are required to, and will take care of, notifying all former and current employees" and that local police service notified former and current employees via email on February 21, 2018. The responsible employee was arrested again sometime between February 3-21, 2018. Between February 23 and March 1, 2018, the Organization sent out several additional notifications to ensure all affected individuals were notified. The Organization reported that on February 21, 2018, the police again informed all current and former employees about the breach.

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 the type of harm that might result from the breach is "identity theft". In my view, the comprehensive identity, financial, educational and profile (background check, residency) information could be used to cause the significant harms of identity theft and fraud. In addition, email addresses could be used for phishing purposes, leading to an increased vulnerability to fraud. 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: *With the assistance of EPS as well as other agencies, the identity of the criminal was discovered quickly. The criminal was arrested. His equipment has been seized, including the hard drive with the employee files. There is no indication he was after employee information. On the contrary, many indications suggest that his motives were in areas that would be damaging to [the Organization] and the CEO/owner specifically (eg: selling information about [the Organization] to the competition, revenge against the CEO, etc).* *There are indications that he was acting alone as revealed by the EPS investigation. There are no indications that additional copies were made…* *Based on the above, there is a low likelihood that harm could result…* *The information was in [the employee's] possession for 10.5 days before his arrest.* 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 malicious action (deliberate intrusion and installation of a keylogger program, copying personal information). The lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach. The information appears to have been exposed for approximately 10.5 days, and I note the police service's notification to affected individuals said "The copy of the computer system that contained your data was seized from the accused on October 6, 2017 but it is unknown if another copy was made or if it was disseminated."

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 comprehensive identity, financial, educational and profile (background check, residency) information could be used to cause the significant harms of identity theft and fraud. In addition, email addresses could be used for phishing purposes, leading to an increased vulnerability to fraud. These are all significant harms. A reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action (deliberate intrusion and installation of a keylogger program, copying personal information). The lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach. The information appears to have been exposed for approximately 10.5 days, and I note the police service's notification to affected individuals said "The copy of the computer system that contained your data was seized from the accused on October 6, 2017 but it is unknown if another copy was made or if it was disseminated." 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 in-person on December 6, 2017 and by email or letter between February 23 and March 1, 2018, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner