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	Trisotech Computer Consulting Services Inc. (Organization)
Decision number (file number)	P2018-ND-150 (File #008175)
Date notice received by OIPC	March 29, 2018
Date Organization last provided information	March 29, 2018
Date of decision	November 16, 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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • business position, • business email address, and • business telephone number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. In addition, the Organization reported that the unauthorized individual(s) may have gained access to: • emails, invoices, contracts, purchase orders, and other information related to sales of software solutions. The Organization reported that all current and potential customers are people interested in business process management (BPM) best practices.

	Given the above, it appears that most, if not all, of the personal information at issue qualifies as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business email address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, to the extent the personal information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 20, 2018, a partner with the Organization received an email requesting invoice payment from an employee. After verbal verification with the employee and his boss, the Organization realized something was wrong. • An internal investigation revealed the Organization had paid a fraudulent invoice on March 12, 2018 and an unauthorised party may have gained access to the Organization's customer management system (CRM system) through one of its employee's accounts. • The unauthorized party may have accessed the system between February 27, 2018 and March 20, 2018. • The Organization reported that none of its computer or network systems were affected by this incident.
Affected individuals	The incident affected 94 individuals residing in Alberta
Steps taken to reduce risk of harm to individuals	• Asked the employee to change his password. • Confirmed that no computers or network systems were affected. • Asked Microsoft for an Access Management Report. • Reviewed current habits and made recommendations to employees.

	• Wrote a check list of security measures to take to reduce the risk of other incidents. • Trained employees. • Notified Chief Security Officer, Police and Canadian Anti-Fraud Centre. • Notified affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 26, 2018.
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 "It is hard to assess the potential harm as we are not sure the unauthorized party managed to copy the data from [the Organization's]) CRM"; however, "We think that there is a potential of fraud. In our notice we have recommended to our clients to contact us if they receive [the Organization's] documents they do not recognize or are not sure of". The Organization also reported "If the unauthorized party would have managed to copy our CRM data, he or she would have the potential of sending fraudulent … invoices to our customers for payment". In my view, the contact information and, in particular, email addresses, in addition to profile information (relationship to the Organization), could be used to send unsolicited emails and for phishing. Consistent with previous breach notification decisions issued by my office, phishing is a significant harm. I also accept the Organization's assessment that the information at issue, in the circumstances, could be used to send fraudulent invoices, which is a significant harm.
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 that "if the unauthorized party …managed to copy our CRM data, he or she would have the potential of sending fraudulent (Organization) invoices to our customers for payment." In my view, the likelihood of harm resulting in this case is increased because the incident appears to be the result of deliberate, malicious action, and related to payment of a fraudulent invoice. Additionally, the information may have been exposed for three weeks.
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 contact information and, in particular, email addresses, in addition to profile information (relationship to the Organization), could be used to send unsolicited emails and for phishing. Consistent with previous breach notification decisions issued by my office, phishing is a significant harm. I also accept the Organization's assessment that the information at issue, in the circumstances, could be used to send fraudulent invoices, which is a significant harm.

The likelihood of harm resulting in this case is increased because the incident appears to be the result of deliberate, malicious action, and related to payment of a fraudulent invoice. Additionally, the information may have been exposed for three weeks.

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 by email on March 26, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner