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	BrandAlliance Inc. (Organization)
Decision number (file number)	P2016-ND-26 (File #002391)
Date notice received by OIPC	February 17, 2016
Date Organization last provided information	March 13, 2016
Date of decision	March 18, 2016
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 operates in Alberta and 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, • credit card number, and • expiry date. This information is about identifiable individuals, and qualifies as "personal information" as defined in section 1(1)(k) of PIPA. Some information was collected in Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On December 11, 2015, the Organization discovered a $5,000 fraudulent transaction and launched an internal investigation. • The investigation found that, using the web interface to the Organization's email system, unauthorized individuals were able to login to a user's email account. • The user had a high level of access to stored credit card data. The email account also contained the wifi password which let the unauthorized individuals connect to the local network. • Once on the local network the unauthorized individuals used credentials and information contained in the user's email account to extract credit card information from what was originally believed to be an in-house account. • The Organization blocked the internet access to this account and the user changed the password. • On January 20, 2016, the Organization was advised by the Ontario police that credit card numbers copied from other databases had been found on a laptop in the possession of thieves. • Subsequently, the police advised that the person of interest who was arrested and charged was a former employee of the Organization and was directly involved in the fraud. • The former employee had intimate knowledge of the entire infrastructure of the Organization's system architecture and helped build the encryption methodology at the time of his employment.
Affected individuals	A total of 25,000, including approximately 2940 Albertans.

Steps taken to reduce risk of harm to individuals	• Reported the incident to the Ontario Police.
	• Reported the incident to the Canadian Anti-Fraud Centre (CAFC).
	• The CAFC advised the Organization that it had:
	  o Referred credit card data of 22,319 cards to 206 financial institutions – this includes all Canadian issued cards.
	  o Notified these financial institutions that the Organization's credit card data is compromised and they are recommended to take appropriate action.
	  o Attempting to establish contact with international banks for 64 outstanding card referrals.
	• Individuals can no longer access the network with a password.
	• The wifi system has been secured using enterprise certificates.

	• Users need to have access to a company computer or have a certificate installed by IT. • The requirements for domain passwords have been strengthened and users are required to change their passwords every 90 days. • Credit card information is deleted once an order has been shipped. • Accelerated the process to move clients to a hosted payment solution where credit card numbers will not pass through or be stored on the Organization's systems. • In the process of auditing systems, networks, policy and procedures.
Steps taken to notify individuals of the incident	The Organization did not notify the affected individuals of the incident. The Organization believes the affected individuals whose credit cards may have been compromised have been "notified through the security department of the issuers of their card association."
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.	In assessing the harm that may result from this breach, the Organization reported: "The credit card information was the only information taken. No SIN's, DOB or drivers's [sic] device information was stored or taken…No bodily harm, damage to reputation loss of employment or opportunities would be reasonably anticipated nor would there be serious threats of identity theft, effect on credit records or damage to or loss of property." I agree with the Organization that the information at issue is unlikely to be used to cause bodily harm, damage to reputation loss of employment or damage to or loss of property. In my view, however, the personal information could be used to cause the harms of identity theft, fraud and financial loss, despite the fact sensitive identity information (such as social insurance number, driver's license number, date of birth) was not involved. In fact, the information compromised in this breach was used to complete a $5,000 fraudulent transaction. These types of harms could also impact an individual's credit records. These are significant harms. As it appears the information involved in this incident was encrypted, I might normally find that the information could not be used to cause significant harm. However, the Organization

	reported that a former employee was involved in the theft and the former employee "was directly involved in our encryption process at the time of his employment."
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 "there is little risk of significant harm through identity theft or liability for fraudulent transactions which would result in financial harm or a negative imptact [sic] on cardholders' credit records." The Organization noted that "[m]ost card assocations [sic] provide holders with fraud protection and have the ability to track and cancel cards with unused or fraudulent activity. Moreoever [sic], we notified the Canadian Anti-Fraud Centre." Finally, the Organization reported that "the thieves who accessed the information have been arrested and the laptop on which the information was stored has been recovered by the police. We have reason to believe that the cards bearing the credit card numbers to which they had access have been cancelled." I am not persuaded by the Organization's submissions. The likelihood of harm resulting from this incident is increased because the personal information was accessed with malicious intent by unauthorized parties, and was exposed for a time before the Organization became aware. The Organization can only speculate but cannot confirm that all affected individuals will be contacted by their credit card issuers or have their cards reissued before any fraudulent transactions occur. It is also speculation that all affected individuals will be reimbursed for fraudulent transactions, even if such transactions are detected. Even though the former employee involved in the fraud has been arrested, it is possible that he made and kept a record of the credit card information, especially given his IT background. The information may even have been further disclosed to other parties. As a result, despite the Organization's submissions, in my view there is a real risk of significant harm resulting from this incident.

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 personal information involved is sensitive financial information that could be used to cause the significant harms of identity theft, fraud and financial loss, and in fact was used to complete a fraudulent transaction. The likelihood of harm resulting from this incident is increased because the personal information was accessed with malicious intent by unauthorized parties. I am not persuaded by the Organization's submissions that the likelihood of harm resulting from this incident is low because credit card issuers will monitor for fraudulent activity, reissue credit cards, and offer fraud protection. The Organization can only speculate but cannot confirm that all affected individuals will be contacted by their credit card issuers or have their cards reissued before any fraudulent transactions occur. It is also speculation that all affected individuals will be reimbursed for fraudulent transactions, even if such transactions are detected. The Organization has submitted that cardholders have already been "notified through the security department of the issuers of their card association". In a previous decision issued by my Office (P2011-ND-001), the former Commissioner stated "PIPA requires the organization having the personal information under its control and which experienced the incident to report the incident and where I determine notification is necessary, to notify the affected individuals." In this case, the Organization had the personal information under its control and experienced the breach, not the credit card issuers. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation), and notify me in writing it has done so on or before April 4, 2016.

Jill Clayton
Information and Privacy Commissioner