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	Tibo Distribution Inc. (Organization)
Decision number (file number)	P2013-ND-42 (File #P2411)
Date notice received by OIPC	August 6, 2013
Date Organization last provided information	September 26, 2013
Date of decision	December 11, 2013
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"	Organization is registered in Quebec. The incident involved a hack of a third party system that operates three Organization websites. I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA and the incident involves personal information provided by Alberta residents through the Organization's website during online purchases.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, and • credit card information (numbers, CCV (credit card verification value) and expiry date). This information is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The online sales system used to facilitate transactions on behalf of the Organization was hacked into exposing the above personal information. The Organization was contacted in April and May of 2013 by its credit card merchant and Amex Canada respectively advising that credit card holders that made purchases from one of the Organization's websites had been compromised. • An internal review of the third party's system used to facilitate sales transactions was conducted and the system was scanned. No evidence of an intrusion on the third party's server was found. • The third party service provider, however, confirmed on July 12, 2013, that its system that contained the above personal information was hacked. • As a result of a forensic investigation, the service provider informed the Organization of the following details about the incident: o The window of intrusion into the system was from May 15, 2012 through July 13, 2013. o The personal information was encrypted; however, it is possible the hacker would have the technical ability to use a decryption feature that could provide access to the name, address, credit card number and expiry date.
Affected individuals	33,588 individuals in Canada potentially affected of which 4,386 are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Technical measures were immediately undertaken to enhance the security of the system. • Credit card information is now purged immediately after the transaction has been completed. • The Organization contacted credit card companies to notify them of the incident who agreed to increase fraud protection for the affected customers.
Steps taken to notify individuals of the incident	Notification was sent to all individuals by email on August 9, 2013.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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 recognized individuals may be at risk for identity theft and fraud, particularly because of the notifications the Organization received from Amex Canada and their credit card merchant that credit cards used on their website had been compromised. In my view, the personal information involved is highly sensitive. The types of harm that could result from unauthorized access to the personal information in this instance are identity theft and fraud. In my view, these are 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 that due to the sensitivity of the personal information involved, it considered there to be a real risk of significant harm to individuals as a result of this incident. In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessed by an unknown third party during a hacking incident. This harm was realized for those individuals whose credit cards were compromised.

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 involves sensitive information. The information has been accessed and used by an unknown third party as a result of a hack. The Organization reported that credit card information used to make purchases on the Organization websites was already compromised. Even though the personal information was encrypted, the Organization was informed by the third party that the hacker may have had the ability to use a decryption feature. These factors contributed significantly to my decision.

I require the Organization to notify the affected individuals from Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by email on August 9, 2013, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals from Alberta again.

Jill Clayton
Information and Privacy Commissioner