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	Boersma Bros LLC, dba DutchWear (Organization)
Decision number (file number)	P2016-ND-53 (File #000118)
Date notice received by OIPC	January 14, 2015
Date Organization last provided information	January 19, 2015
Date of decision	August 26, 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 is an "organization" as defined in section 1(1)(i)(i of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • credit card number, • expiration date, and • CVV2 (card verification) code This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• An unknown entity installed malicious software on the Organization's online purchasing system. • The malware intercepted (accessed) personal information of customers who made online purchases between November 7, 2014 and December 6, 2014.
Affected individuals	There were 8 affected individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• The e-commerce site was isolated and an investigation was conducted. • The Organization reported that the compromised site was decommissioned and steps were taken to develop and implement a new site with improved security controls.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter.
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 "credit card information can be used to make fraudulent charges on customer's accounts." I agree with the organization. The information at issue could be used to cause the harms of identity theft, fraud and financial loss. 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 "the likelihood of harm is low" and noted that "Misuse of credit card information is usually recognized as a significant harm, although we note that consumers are typically not responsible for unauthorized charges made under these circumstances." In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessed in an unauthorized manner with malicious intent, and was exposed for approximately a month. The Organization can only speculate that affected individuals would not be held responsible for any fraudulent charges. Even if this were the case, it only addresses credit card fraud and would not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the personal information was accessed in an unauthorized manner with malicious intent, and was exposed for approximately a month. The Organization can only speculate that affected individuals would not be held responsible for any fraudulent charges. Even if this were the case, it only addresses credit card fraud and would not necessarily mitigate the potential harm from identity theft or other forms of fraud. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individuals via letter in accordance with the Regulation. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner