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	Scripps Networks, LLC (Organization)
Decision number (file number)	P2017-ND-22 (File #001801)
Date notice received by OIPC	October 16, 2015
Date Organization last provided information	February 2, 2016
Date of decision	January 30, 2017
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 a U.S. corporation and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • email addresses/usernames, • passwords, and • date of birth (or possibly month and year of birth). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's e-commerce website, Food.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On August 31 2015, the Organization received a message from an individual claiming he had identified a vulnerability in the Organization's Food.com website that allowed him to access certain personal information of the website's users. • The Organization investigated and, on September 16, 2015, determined that an intruder had accessed the Organization's system between August 8, 2015 and September 2, 2015. • The intruder may have had unauthorized access to, and potential acquisition of, some customer personal information.
Affected individuals	The incident potentially affected 17,115 Canadians. The Organization is unable to determine precisely how many of these individuals are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged a forensic investigator to analyze the incident. • Took steps to ensure this type of intrusion will not happen again and to protect against other types of intrusion. • Advised affected individuals to change their passwords.
Steps taken to notify individuals of the incident	Individuals potentially affected by this incident were notified by email sent October 16, 2015.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 its report of the incident, the Organization noted that the information at issue (credentials) could be used to access various of the Organization's user accounts as well as mobile applications. In its notification to potentially affected individuals, the Organization provided information about updating/changing passwords and being alert to possible phishing attacks. In my view, the credential information at issue could be used for phishing purposes and to access other accounts where affected individuals may have used the same login credentials. 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 did not specifically assess the likelihood of harm resulting from this incident. In my view, the likelihood of harm is increased as the breach was the result of malicious intent (deliberate intrusion and exfiltration) and the information was exposed for approximately 3 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 as a result of this incident. The credential information at issue could be used for phishing purposes and to access other accounts where affected individuals may have used the same login credentials. These are significant harms. The likelihood of harm is increased as the breach was the result of malicious intent (deliberate intrusion and exfiltration) and the information was exposed for approximately 3 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 that written notice of the incident was emailed to affected individuals on October 16, 2015. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner