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	The Canadian Kennel Club (the Organization)
Decision number (file number)	P2019-ND-077 (File #011967)
Date notice received by OIPC	February 7, 2019
Date Organization last provided information	February 7, 2019
Date of decision	June 4, 2019
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 whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a non-profit organization incorporated under the Animal Pedigree Act of Canada. It is not a non-profit organization as defined in PIPA, such that PIPA would only apply to personal information collected in connection with the Organization's commercial activities. Instead, the Organization is an "organization" as defined in section 1(1)(i) of PIPA, to which PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The incident involved files compiled during discipline or appeal processes which contained the following classes of information: • names of individuals subject to a proceeding and of complainants (in some cases); • complaint allegations, response, filings and written arguments of the parties to the proceeding, including witness statements; • correspondence; • decisions of the Registration, Discipline and Appeal Committees; • contact information for individuals subject to proceedings and witnesses; • registered names, numbers and identification of dogs (which is publicly available), together with information regarding the ownership of such dog, including the owner's name and contact information (not typically made public).

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On December 1, 2018, a former member of the Discipline Committee reported being able to access a discipline file following a search on the Organization's public website. • The Organization's IT group determined that disciplinary, appeals and registration files could be accessed through the 'search' functionality on the public website. • An investigation found that the breach occurred in June 2018 when the Organization implemented a new website and, due to human error, the accessibility settings were incorrectly set. • The potential for access to the files through the public website lasted from June 2018 until the security settings were reset on December 3, 2018.
Affected individuals	The incident affected approximately 191 individuals, including 40 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Corrected the issue within 48 hours and ended access from the public website. • Investigated to determine the cause of the incident, and impact on files potentially accessed.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent between February 4-7, 2019.
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 "…there is the potential for unauthorized access to the Files to result in harms such embarrassment, damage to reputation, and loss of business opportunities". In my view, a reasonable person would consider the information at issue could be used to cause the significant harms of hurt, humiliation and embarrassment, and potentially damage to reputation.

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 it "… has determined that there is a real risk of significant harm to the affected individuals; there is a potential for embarrassment, damage to reputation, and loss of business opportunities. However, the risk that this harm will materialize is lowered by the fact that the the [sic] information was not published on the website in a manner that rendered it easily visible to the public. The Files and the information could be found on the website only following a search using the website's 'search' functionality or by entering the URL of the File directly. Further, the incident arose from human error and there is no evidence of any malicious activity". In my view, a reasonable person would consider that the likelihood of harm is reduced because the breach did not result from malicious intent. I also accept the Organization's assertion that the information might not be readily found. However, it is not clear from the Organization's report how many individuals may have accessed the information, nor any technical controls (such as audit logs) that could evidence that the information was not accessed. It appears the information was exposed for close to 6 months.

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.

A reasonable person would consider the information at issue could be used to cause the significant harms of hurt, humiliation and embarrassment, and potentially damage to reputation. The likelihood of harm is reduced because the breach did not result from malicious intent. I also accept the Organization's assertion that the information might not be readily found. However, it is not clear from the Organization's report how many individuals may have accessed the information, nor any technical controls (such as audit logs) that could evidence that the information was not accessed. It appears the information was exposed for close to 6 months.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand affected individuals were notified by letter sent between February 4-7, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner