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	D+H Limited Partnership (Organization)
Decision number (file number)	P2018-ND-029 (File #000966)
Date notice received by OIPC	May 8, 2015
Date Organization last provided information	May 8, 2015
Date of decision	March 19, 2018
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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization is a financial technology services company that offers a service called CreditDefend, a credit monitoring service that, among other things, provides individuals with the ability to obtain an online copy of their own credit report. These credit reports are maintained by Equifax Inc. Individuals wishing to access their credit report can only do so if they authenticate through Equifax. The Organization reported that "…an unauthorized third party (or parties) may have gained access to the credit reports of individuals. In order to have done so, the unauthorized third party (or parties) must have previously obtained the necessary personal information to pass the authentication process. Specifically, the necessary authentication information includes an individual's name, address and date of birth, as well as their personal financial information, such as mortgage amount, the institution that holds the mortgage, the amount of the last credit card payment, or the last piece of credit applied for. In short, it would appear that the affected individuals may have already been victims of identity theft or some sort of privacy breach in order for the third-party to be in possession of the necessary identity authentication information."

	Name, address, date of birth, and financial information is information about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. It is not clear from the report submitted to my office, or communications with the Organization, that the Organization is the entity in control of the information with the legal obligation to report the breach to my office. To the extent the Organization had control of the information at issue and collected the information in Alberta, I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On February 17, 2015, an individual contacted the Organization to ask why there was an inquiry from CreditDefend that appeared on the individual's credit report. • The Organization investigated and determined that a CreditDefend account had been opened in the individual's name by an unauthorized individual, but safeguards prevented access to the requested credit report through CreditDefend. • The investigation also revealed "…that 39 individuals, across Canada, may have been affected" and "Four (4) of those individuals reside in Alberta. The CreditDefend accounts for these individuals were all activated on or about January 12, 2015. By March 12, 2015, all of the potentially affected CreditDefend accounts (including the four (4) CreditDefend accounts of individuals resident in Alberta) had been deactivated".
Affected individuals	The incident affected 39 Canadians, including 4 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Suspended public access to the consumer-facing online sales channel. • Determined which individuals were affected by the incident and deactivated the accounts to prevent further access. • Conducted an investigation and liaised with Equifax as appropriate. • Notified affected individuals. • Offered reimbursement for expenses associated with placing credit card alerts on credit reports. • Opened a call centre line to assist affected individuals. • Commenced a full review of the relevant policies and protocols associated with the incident.

Steps taken to notify individuals of the incident	Affected individuals were notified by letter on May 6, 2015.
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 "the personal information involved in this incident is sensitive and could be used to perpetrate identity theft and fraud. Given the individual's ability to properly answer the questions asked during the [Organization's] stringent authentication process, it appears that the perpetrator had already acquired the affected individual's sensitive personal information. We believe that the affected individuals may have already been a victim of a privacy breach or identity theft." I agree with the Organization. The identity, contact and financial information that may be at issue could be used to cause the significant harms of identity theft, fraud and financial loss.
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 provide an assessment of the likelihood that significant harm would result from this incident. In my view, the likelihood of harm is increased because the incident was a result of malicious intent (deliberate unauthorized action) and the personal information may have been exposed for approximately two 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. The identity, contact and financial information that may be at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm is increased because the incident was a result of malicious intent (deliberate unauthorized action) and the personal information may have been exposed for approximately two months. The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals in a letter dated May 6, 2015 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.	

Jill Clayton
Information and Privacy Commissioner