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	DealerTrack Canada Inc. (Organization)
Decision number (file number)	P2014-ND-09 (File #P2637)
Date notice received by OIPC	March 26, 2014
Date Organization last provided information	March 26, 2014
Date of decision	August 5, 2014
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 corporation operating in Alberta. The incident occurred in Alberta. I have jurisdiction because 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 about the individuals: • Full name • Full address • Phone number (home) • Social insurance number (last three digits) • Date of birth • Gender • Marital Status • Email address • Duration of residence at current address • Previous address

	• Home ownership status • Mortgage details, including payment amount • Current employment information, including employer, length of service, and employment status • Income details • For one individual, the full social insurance number (beyond the last three digits) was accessed This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ☒ unauthorized disclosure	
Description of incident	• A successful social engineering attack was carried out on October 13, 2013, targeting Toyota City, Wetaskiwin, Alberta. • Toyota City uses the DealerTrack application managed by DealerTrack Canada Inc. • An attacker called an employee of Toyota City while impersonating an employee of DealerTrack Canada Inc. • The attacker requested and obtained the Toyota City employee's authentication credentials (user ID, PIN and security questions) for the DealerTrack application. • The compromised account was an administrative (i.e. privileged) account. • The attacker used the compromised administrative account to access personal, financial and employment information of individuals from three different lending organizations. • The attacker also used the privileges of the compromised account and created a generic account. • The attacker unsuccessfully attempted to use the generic account to access similar information.
Affected individuals	• Four
Steps taken to reduce risk of harm to individuals	• The compromised account of the Toyota City employee was disabled and a new one created. • The generic account created by the attacker was removed. • Using displayed messages on auto dealer terminals, DealerTrack Canada Inc. has educated users regarding social engineering attacks. • Individuals affected by the incident were advised to monitor their credit records.

Steps taken to notify individuals of the incident	• A notification letter was sent to each of the individuals affected by the incident. • The letters were sent by Toyota City, Wetaskiwin, on March 5, 2014.
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 that the affected individuals may be at risk of harm. In my view, the personal, financial and employment information involved is highly sensitive. The types of harm that could result from unauthorized access to or use of the information in this instance are identity theft, financial loss and/or fraud.
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.	Due to the sensitivity of the personal, financial and employment information involved there are real risks of significant harm to the affected individuals. In my view, the likelihood of harm resulting from this incident is increased because the personal information is sensitive and was accessed by, at least, one unauthorized individual.
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 personal, financial and employment related information and was accessed by an unauthorized individual with malicious intent. These factors contributed significantly to my decision. 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, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.	

Jill Clayton
Information and Privacy Commissioner