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	Manulife Financial (Organization)
Decision number (file number)	P2017-ND-25 (File #001907)
Date notice received by OIPC	December 2, 2015
Date Organization last provided information	March 7, 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 incorporated in Alberta and 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, • customer identification number, • Social Insurance Number, • date of birth, • name of employer, and • name of beneficiary. 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.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• In April 2015 the Organization received a complaint from a client which prompted an internal audit. • The audit found that unknown individuals purchased personal information from an employee of the Organization (now former employee) and used that information to call in to the Organization, authenticate as members and gain access to online accounts. The unauthorized individuals changed member banking information, requested withdrawals be directed to fraudulent bank accounts, and submitted forged withdrawal request forms and Home Buyers Plan forms. • A suspect was identified in July 2015.
Affected individuals	Approximately 15 Alberta clients were affected by this incident.
Steps taken to reduce risk of harm to individuals	• Client accounts are being monitored and made whole. • Credit monitoring services provided to affected individuals. • Notified law enforcement and former employee has been arrested and charged. • Enhanced administrative, technical and physical controls.
Steps taken to notify individuals of the incident	Affected individuals were notified between June 25, 2015 and January 2016.
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 "The level of information compromised is assessed to be high risk information. The information was used for unauthorized access to client accounts with intent to cause financial harm to [the Organization's] clients." Further, "The theft of personal information was intended to be used for identity theft to take over … client accounts." In my view, the information at issue includes contact, identity and financial information that 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 that the theft of personal information was "intended to be used for identity theft" and noted that the "Information was exposed during time frame of April 2015 – July 2015." The Organization also reported that it "has taken action for impacted clients, making accounts and extra protection controls on accounts along with credit monitoring services."

	In my view there is a real risk of significant harm resulting from this breach. The incident is the result of deliberate action with intent to commit identity theft, and the information was exposed for at least three months. The Organization did not confirm the personal information was not copied or forwarded on to other parties (i.e. the information is not recovered). Finally, the information was used to commit fraudulent acts.

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 includes contact, identity and financial information that could be used to cause the significant harms of identity theft, fraud and financial loss. The incident is the result of deliberate action with intent to commit identity theft, and the information was exposed for at least three months. The Organization did not confirm the personal information was not copied or forwarded on to other parties (i.e. the information is not recovered). Finally, the information was used to commit fraudulent acts.

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 between June 25, 2015 and January 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner