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	General Motors Financial Company Inc. (Organization)
Decision number (file number)	P2017-ND-57 (File #001387)
Date notice received by OIPC	August 14, 2015
Date Organization last provided information	August 14, 2015
Date of decision	May 15, 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 operates 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 all or some of the following information: • customer contact information, • date of birth, • social insurance number, • bank account information, and • an image of the customer's driver's license. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information was collected from residents of Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 20, 2015, the Organization was notified by local law enforcement that print-outs from its customer files had been found in a stolen vehicle. A total of 8 customer files were found.

	• The Organization investigated and determined an employee improperly accessed the customer files identified by police. • The Organization also determined that the employee accessed other customer files over a span of approximately 7 years. • On June 4, 2015, the Organization became aware that residents of Alberta were affected. • The employee was terminated.
Affected individuals	The incident affected 2200 individuals, of which 122 were residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Revoked employee's systems and building access. • Terminated the employee. • Notified the Organization's Privacy Officer. • Notified all affected individuals. • Issued a press release on July 29, 2015 relating to the breach. • Offered credit monitoring services and identity theft insurance to all affected individuals. • Committed to reimbursing affected individuals for financial losses suffered as a direct result of the breach.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail sent on August 10, 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.	In its report of the incident, the Organization advised that "Each… customer file contains information that is sensitive from a personal and financial perspective, which, if inappropriately accessed and used, could be involved in identity theft or fraud." I agree with the Organization. Identity and financial information could be used to cause identity theft and fraud. Customer contact information could be used to gain unauthorized access to other accounts and could be used for phishing purposes. 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 significant harm could result due to the type and sensitivity of the information involved and because "the fact that the former employee has both confessed to improperly accessing and disclosing [the Organization's] customer files and been charged by [law enforcement] with making identity information available for a fraudulent purpose in contravention to the *Criminal* Code of *Canada…".*

	I agree with the Organization's assessment. The likelihood of harm resulting from this incident is significantly increased because the personal information was compromised due to the malicious actions of a former employee (deliberate action for fraudulent purposes). The employee accessed customer files over a span of approximately 7 years, confessed to improper access and disclosure, and was charged with making identity information available for a fraudulent purpose.

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. Identity and financial information could be used to cause identity theft and fraud. Customer contact information could be used to gain unauthorized access to other accounts and could be used for phishing purposes. These are significant harms. The likelihood of harm resulting from this incident is significantly increased because the personal information was compromised due to the malicious actions of a former employee (deliberate action for fraudulent purposes). The employee accessed customer files over a span of approximately 7 years, confessed to improper access and disclosure, and was charged with making identity information available for a fraudulent purpose.

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 the Organization notified affected individuals in an email dated August 10, 2015, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner