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	National Money Mart Company (Organization)
Decision number (file number)	P2017-ND-91 (File #P2788)
Date notice received by OIPC	July 31, 2014
Date Organization last provided information	November 18, 2015
Date of decision	July 14, 2017
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Canada, including 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 about the affected individual: • name, • address, • date of birth, • Social Insurance Number (SIN), • telephone number, • email address, • driver's license number, • birth certificate number, • employment information (name of employer, job title, length of employment and net pay), and • reference information (name of parent and name of friend, and contact telephone numbers for both). This information is about an identifiable individual in Alberta and is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On July 14, 2014, an individual entered one of the Organization's stores in British Columbia purporting to be a customer of the Organization. The individual requested a copy of her customer transaction history and registration form, and provided a social insurance card and native status picture ID card as identification. • A clerk reviewed the identification, matched the information with the Organization's records, and proceeded with the transaction. The information at issue was provided to the individual. • On July 16, 2014, the Organization was notified by the RCMP that the individual had been taken into custody. The individual was identified by the Organization's staff as being the person who appeared in the store on July 14, 2014 and obtained the information at issue, after representing herself as a customer of the Organization. • The Organization believes that the affected customer's personal information was breached prior to the July 14 incident and that the individual apprehended by the RCMP had earlier attempted to obtain an on-line loan under the name of the affected customer.
Affected individuals	The incident affected one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Increased monitoring of transactions on affected customer's account. • Reviewed the transaction with the clerk and took appropriate action, including providing remedial training on Privacy Policies and Procedures. • Working with affected customer to obtain a new social insurance number as the original was compromised.
Steps taken to notify individuals of the incident	The affected customer (individual) was notified by telephone on July 18, 2014.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 this incident the Organization said it believed the individual "attempted to defraud [the Organization]" and obtain information necessary to apply for an on-line loan under the name of the affected customer. In my view, the contact, identity, and employment information involved could be used to cause the harms of identity theft, fraud and financial loss. Email address could be used for phishing purposes. These are all 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 "Given [the individual] was taken into custody by the RCMP, we believe the likelihood that harm will result is low. There was no financial loss to [the affected customer]…". In my view, there is a real risk of harm in this case. The incident resulted from malicious intent (use of someone else's identification to deliberately and fraudulently obtain personal information with an eye to committing financial fraud). Although the perpetrator has been apprehended, the Organization did not report that the information has been recovered. It may be that there are enhanced safeguards to prevent further fraudulent activity at the Organization's locations; however, the information at issue could be used for identity theft and fraud in other circumstances.

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 individual. The contact, identity, and employment information involved could be used to cause the harms of identity theft, fraud and financial loss. Email address could be used for phishing purposes. These are all significant harms. The incident resulted from malicious intent (use of someone else's identification to deliberately and fraudulently obtain personal information with an eye to committing financial fraud). Although the perpetrator has been apprehended, the Organization did not report that the information has been recovered. It may be that there are enhanced safeguards to prevent further fraudulent activity at the Organization's locations; however, the information at issue could be used for identity theft and fraud in other circumstances.

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 individual by telephone on July 18, 2014. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner