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	HollisWealth, a division of Scotia Capital Inc. (Organization) This incident was reported by Scotiabank, on behalf of its subsidiary, Scotia Capital Inc.
Decision number (file number)	P2015-ND-73 (Case File #P2758)
Date notice received by OIPC	May 6, 2014
Date Organization last provided information	May 13, 2014
Date of decision	November 5, 2015
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"	Scotiabank reported that the Organization is an agent of Scotiabank, operating as an independent franchisee. The Organization retains control of customer financial information. The Organization is incorporated in Alberta, and qualifies as 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, • social insurance number (SIN), • date of birth, • address, • telephone number, • financial information, • employment information, • signature, • copy of driver's licence or other government identification.

	This information is about identifiable individuals, and qualifies as "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	• The Organization's office was broken into on April 8, 2014. Several items were stolen, including two laptops, three portable hard drives used for back-up purposes, and several USB memory sticks. • The stolen devices were not encrypted.
Affected individuals	580 individuals were affected by the incident.
Steps taken to reduce risk of harm to individuals	• Reported the theft to law enforcement, the Privacy Commissioner of Canada, and the Office of the Superintendent of Financial Institutions. • Reported to internal compliance. • Commenced an internal investigation. • Several initiatives underway to provide technology support and enhanced safeguards (encryption).
Steps taken to notify individuals of the incident	• Notified all affected individuals by mail. • Offered one year of credit monitoring to affected individuals.
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 is sufficient for purposes of identity theft. I agree with the Organization. The personal information involved is sensitive and contains identity and financial information. This information could be used to cause the harms of identity theft and fraud. 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 although it believes the incident was a theft of opportunity, the information was not encrypted. In my view, the likelihood of harm is increased because the incident was the result of malicious intent (a break-in and theft). The mobile devices were not encrypted.

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 affected individuals. The personal information could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (a break-in and theft) and the mobile devices were not encrypted.

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 individuals affected by the incident in accordance with section 19.1 of the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner