



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	HSBC InvestDirect, a division of HSBC Securities (Canada) Inc. (Organization)
Decision number (file number)	P2019-ND-059 (File #008537)
Date notice received by OIPC	May 1, 2018
Date Organization last provided information	February 13, 2019
Date of decision	May 6, 2019
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 <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• mailing address,• account number,• social insurance number (SIN),• income/tax amount, and• total market value of account holdings. <p>This information is about an identifiable individual and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
DESCRIPTION OF INCIDENT	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On April 3, 2018, a client contacted the Organization to complain that his T4RSP and annual report had been sent to the wrong address.• The Organization discovered the client’s mailing address had been updated incorrectly on March 28, 2017.

	<ul style="list-style-type: none"> • The Organization requested that the unauthorized recipient return the documents to the Organization or shred them and confirm with the Organization when he/she did so. However, the Organization did not obtain said confirmation. • The information has not been recovered.
Affected individuals	The incident affected one (1) individual residing in Alberta
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Offered to change the client’s account number. • Followed up at the inaccurate address, but was unable to obtain confirmation of secure destruction or the recovery of the documents. • Enrolled affected individual in a one year of credit monitoring and protection at the Organization’s expense.
Steps taken to notify individuals of the incident	The affected individual was notified verbally in accordance with the PIPA Regulations on April 3, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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.</p>	<p>The Organization reported “The disclosure of the client’s name, address and social insurance number (SIN) to unauthorized parties could result in identity theft and/or fraud.”</p> <p>I agree with the Organization’s assessment. A reasonable person would consider that the contact, financial and identity information at issue could be used to cause the significant harms of identity theft and/or fraud.</p>
<p>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.</p>	<p>The Organization reported that it believes “the likelihood of imminent harm to be lessened due to the following factors”:</p> <ul style="list-style-type: none"> - “We are aware of the address the tax slips and annual report where sent to”. - “The client is eligible to enrol for a one-year term of credit monitoring and protection at the [Organization’s] expense”. - “We have offered to change the client’s ... account number, but client (sic) does not want to change it”. - “A letter was sent to the residents [of the inaccurate address] ...asking them to return the documents ... or shred them and asking them to contact us to confirm they did so”. - “Although the disclosed information could result in identity theft and/or fraud, we have no evidence the information has been used for these purposes”. <p>In my view, although the incident resulted from human error and not malicious intent, the Organization was not able to recover the</p>

	documents, or confirm that the personal information was destroyed securely. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach.
--	--

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.

A reasonable person would consider that the contact, financial and identity information at issue could be used to cause the significant harms of identity theft and/or fraud. Although the incident resulted from human error and not malicious intent, the Organization was not able to recover the documents, or confirm that the personal information was destroyed securely. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach.

I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual verbally in accordance with the Regulation on April 3, 2018. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner