



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	HSBC InvestDirect (Organization)
Decision number (file number)	P2020-ND-119 (File #013654)
Date notice received by OIPC	August 8, 2019
Date Organization last provided information	August 8, 2019
Date of decision	October 27, 2020
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 whose personal information was collected in Alberta pursuant to section 37.1 of <i>the 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 the following information:</p> <ul style="list-style-type: none">• name,• mailing address,• social insurance number,• taxable income from RRIF,• mutual fund trade details. <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 type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• Due to a system misconfiguration, the Organization inadvertently mailed a customer’s mutual fund confirmation slip and T4RIF to the wrong address.• The errors occurred on January 23, 2019 and February 5, 2019.

	<ul style="list-style-type: none"> The errors were discovered on March 13, 2019 when the customer contacted the Organization.
Affected individuals	The incident affected one (1) individual.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Provided two-year complementary credit monitoring and protection. Offered to change the client's account number and verbal/online passwords. Sent a letter to the unauthorized recipient on April 9, 2019, requesting the return of the documents or confirmation of shredding.
Steps taken to notify individuals of the incident	The Organization reported the affected individual notified the Organization of the breach on March 13, 2019 and the Organization offered various remedies to address potential harm(s) that might result from the breach.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>Harm</p> <p>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 identify theft and/or fraud."</p> <p>In my view, a reasonable person would consider the contact, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud.</p>
<p>Real Risk</p> <p>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:</p> <p><i>Although we have determined the disclosed information to be of a highly sensitive nature, we believe the likelihood of imminent harm to be lessened due to the following factors:</i></p> <p><i>We are aware of the address the tax slip and mutual fund confirmation slip where sent to.</i></p> <p><i>The client has signed up for a two-year term of credit monitoring and protection...</i></p> <p><i>We have offered to change the client's ... account number and verbal/on line passwords, but client does not want to change them.</i></p> <p><i>A letter was sent to the residents of the wrong address April 9th, 2019, asking them to return the documents to a</i></p>

	<p><i>local HSBC branch or shred them and asking them to contact us to confirm they did so.</i></p> <p><i>Although the disclosed information could result in identity theft and/ or fraud, we have no evidence the information has been used for these purposes.</i></p> <p>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is decreased because it resulted from human error and not malicious action. However, although the Organization wrote to the unintended recipient requesting the return of the documents or confirmation of secure destruction, the Organization did not report receiving such confirmation.</p>
--	--

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 the contact, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is decreased because it resulted from human error and not malicious action. However, although the Organization wrote to the unintended recipient requesting the return of the documents or confirmation of secure destruction, the Organization did not report receiving such confirmation.

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

I understand the affected individual reported the incident to the Organization on March 13, 2019 and the Organization offered various remedies to address potential harm(s) that might result from the breach. Given this, the Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner