



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)	P2017-ND-109 (File #006107)
Date notice received by OIPC	July 18, 2017
Date Organization last provided information	July 18, 2017
Date of decision	August 4, 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 the individuals 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 a self-directed, online investing brokerage and is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The Organization reported the incident involved the following information as contained in such documents as trading summaries, investment income summaries, T5s, T5008/R18s, performance reports and others:</p> <ul style="list-style-type: none">• name,• date of birth,• address,• account number,• social insurance number,• account balances, and• transaction information. <p>This information is about identifiable individuals 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	

<p>Description of incident</p>	<ul style="list-style-type: none"> • A husband and wife (the clients) set up an account with the Organization in 2015. When the account was opened, the address on the application was correct but was entered into the Organization’s system incorrectly as a result of human error. • On May 11, 2017 an individual brought two documents into one of the Organization’s branches and asked staff to stop mailing documents to his address. The individual stated he threw out previous mail he received for the clients and that he had raised this issue on his last visit stating he'd been receiving the clients' mail for around a year.
<p>Affected individuals</p>	<p>The incident affected two (2) individuals.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<p>Corrected the address in the system.</p>
<p>Steps taken to notify individuals of the incident</p>	<p>The Organization notified the affected individuals in person and writing on May 30, 2017.</p>
<p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p>	
<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 that “Based on the information breached ... the following types of harm may result - Fraud and/or identity theft”.</p> <p>I agree with the Organization. The contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. These are significant harms.</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 considered the following factors in assessing the likelihood of harm resulting from this incident:</p> <ul style="list-style-type: none"> • “We have lost control of sensitive data.” • “Because the information was sent by way of paper documents to the wrong address, there were no security measures in place to prevent unauthorized access once the paper documents left [the Organization’s] premises.” • “The individuals affected are seniors.” <p>In my view, there is a real risk of significant harm in this case. Although the incident resulted from human error and not malicious intent, “multiple” documents containing sensitive personal information were sent to an unauthorized recipient over a period of two years. The documents have not been recovered.</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 individuals in this case.

The contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. These are significant harms. Although the incident resulted from human error and not malicious intent, “multiple” documents containing sensitive personal information were sent to an unauthorized recipient over a period of two years. The documents have not been recovered.

The Organization is required to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individuals were notified in person and writing on May 30, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner