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	HSBC Investment Funds Inc. (Organization)
Decision number (file number)	P2021-ND-296 (File #020310)
Date notice received by OIPC	January 26, 2021
Date Organization last provided information	October 13, 2021
Date of decision	March 2, 2022
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 information was collected in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (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"	The incident involved some or all of the following information: • full name, • address, • social insurance number, • account number, and • account details, including contribution and payment amounts. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• The Organization's customer agreements require customers to keep their contact details up to date, including their mailing address. From time to time, mail sent by the Organization to customers at their address on file is returned to sender. On the basis that such customers have not updated their mailing address, the Organization will place a return mail flag on their accounts

	directing that mail not be sent to their address until such time as their address has been updated ("return mail flag"). • Between February and March 2020, due to a system error, the Organization sent 2019 tax slips to the holders of accounts with return mail flags on them (sent to the last address noted on the customer account). • An individual, who was not a customer, informed the Organization that they received mail for a customer with the Organization.
Affected individuals	The incident affected one (1) individual whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Updated customer addresses; • Offered affected individuals complimentary credit alert identity protection services for two years and recommended that they contact major credit bureaus to place alerts on their credit files; • Reminded affected individuals to keep their contact information up to date; and • Introduced a new process related to its tax slip production.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and by letter on January 27, 2021.
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 possible harms that may occur as a result of the breach is "Unathorized (sic) use of personal information". In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud.
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 assessed the likelihood of harm resulting from this incident as follows: *Medium - breached information is highly sensitive but we are aware that it went to the customer's old address. We have not received any customer complaints and customers will be offered free credit monitoring services for two years.* In my view, a reasonable person would consider that the likelihood of harm is decreased because the breach did not result from malicious intent, but rather human error. However, it is unclear whether the Organization requested that unintended recipients return the information to the Organization, or that the information be destroyed, and not forwarded, re-distributed, or copied, etc. The lack of reported incidents 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, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm is decreased because the breach did not result from malicious intent, but rather human error. However, it is unclear whether the Organization requested that unintended recipients return the information to the Organization, or that the information be destroyed, and not forwarded, re-distributed, or copied, etc. The lack of reported incidents to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. The Organization is required to notify the affected individual whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation*. I understand that affected individual was notified by telephone and letter on January 26, 2021. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner