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	Olympia Trust Company (Organization)
Decision number (file number)	P2017-ND-154 (Case File #006938)
Date notice received by OIPC	October 24, 2017
Date Organization last provided information	October 24, 2017
Date of decision	November 24, 2017
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 *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is incorporated in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • date of birth, • Social Insurance Number, • email address, • telephone number, • signature. This information is about an identifiable individual and is "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	• On October 13, 2017, an employee of the Organization mistakenly emailed an account opening application to the wrong client.

	• The Organization discovered the incident on October 14, 2017 when the unintended recipient reported the error.
Affected individuals	The incident affected one (1) individual in Alberta.
Steps taken to reduce risk of harm to individuals	Revised practices and no longer automatically forwards account opening applications to clients opening accounts.
Steps taken to notify individuals of the incident	The affected individual was contacted by telephone.
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 information at issue "could all be used for identity theft purposes. This is turn could result in financial loss and a negative effect on the client's credit rating." I accept the Organization's assessment. The identity and financial information could be used to cause the harms of identity theft, fraud, financial loss and a negative effect on credit rating. Email address could be used for phishing purposes. 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 its assessment that "it is unlike [sic] that the clients affected by this breach will experience any harm as a result of this breach. The unauthorized disclosure of personal information was reported by the individual who received the information. The individual that received the information received the information in an accidental manner and was not actively seeking the information. Accordingly, it is unlikely that the individual who received the information has any nefarious or malicious intentions." I agree with the Organization that the likelihood of harm resulting from this incident is reduced because the incident resulted from human error, rather than malicious intent, and the unintended recipient reported the error. However, the Organization did not report any efforts to confirm with the unintended recipient that the information was not used or shared, and that it was destroyed.
DECISION UNDER SECTION 37.1(1) OF PIPA	
Given the information reported by the Organization, I have concluded that there is a real risk of harm in this case.	

The identity and financial information could be used to cause the harms of identity theft, fraud, financial loss and a negative effect on credit rating. Email address could be used for phishing purposes. These are significant harms. The likelihood of harm resulting from this incident is reduced because the incident resulted from human error, rather than malicious intent, and the unintended recipient reported the error. However, the Organization did not report any efforts to confirm with the unintended recipient that the information was not used or shared, and that it was destroyed.

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

I understand the Organization notified the affected individual by telephone. The Organization is not required to do so again.

Jill Clayton
Information and Privacy Commissioner