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	Future Values Estate and Financial Planning (Organization)
File number	P2017-ND-15 (File #001074)
Date notice received by OIPC	June 25, 2015
Date Organization last provided information	June 25, 2015
Date of decision	January 9, 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 an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name, • date of birth, • address, • telephone number, • Social Insurance Number, • email address, • client identification number, and • RRSP account number. 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 June 4, 2015, an email containing the personal information at issue was sent to a client's correct email address, but also copied to an incorrect email address. • The incident was discovered on June 9, 2015, when the client reported the email was sent to an incorrect email address and expressed concern that someone else may have access to his personal information.
Affected individuals	The incident affected one (1) individual.
Steps taken to reduce risk of harm to individuals	• The email was not encrypted, but contained a notice requesting any unintended recipients to notify the sender and delete or destroy the communication. • The Organization placed warning flags on the client's investment and insurance accounts. • The incident was reported to a number of internal compliance officers.
Steps taken to notify individuals of the incident	The Organization notified the affected individual by telephone and email correspondence beginning June 9, 2015.
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 is sensitive and "Harm may be significant in the event of potential identity theft." I agree with the Organization's assessment. The personal information includes sensitive identity and financial information that could be used to cause the harms of identity theft and fraud. 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 a "Low risk level due to prompt discovery and subsequent actions taken to safeguard client's accounts." The Organization also noted that the information was exposed for "Up to 5 days before client alerted me to incorrect email address" and that, although there is no evidence of unauthorized attempts to access the affected individual's client account, the "email was not able to be retracted."

	In my view, although the incident was the result of human error and not malicious intent, the likelihood of harm resulting from this incident is increased because the Organization did not report contacting the unintended recipient, nor confirming that the unintended recipient did not access, copy or disclose the personal information. Although steps were taken to secure the client's accounts, this does not necessarily mitigate the risk that the personal information at issue will be used for identity theft or other forms of fraud in other transactions.

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 to the affected individual in this case. The personal information includes sensitive identity and financial information that could be used to cause the harms of identity theft and fraud. These are significant harms. Although the incident was the result of human error and not malicious intent, the likelihood of harm resulting from this incident is increased because the Organization did not report contacting the unintended recipient, nor confirming that the unintended recipient did not access, copy or disclose the personal information. Although steps were taken to secure the client's accounts, this does not necessarily mitigate the risk that the personal information at issue will be used for identity theft or other forms of fraud in other transactions.

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

I understand the Organization notified the affected individual by telephone and email correspondence beginning June 9, 2015. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner