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	Wealthbridge Financial Services Inc. (Organization)
Decision number (file number)	P2021-ND-146 (File #017482)
Date notice received by OIPC	May 27, 2020
Date Organization last provided information	May 27, 2020
Date of decision	June 2, 2021
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 *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 all or some of the following information: • name, • net worth, • bank address, • account number, • investment account number, and • 2020 personal income tax position forecast. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☐ loss ☐ unauthorized access	☒ unauthorized disclosure
Description of incident	• On May 15, 2020, an employee with the Organization emailed a draft document containing the personal information at issue to an unintended recipient. • The employee mistyped the intended email address and accidentally sent the document to an incorrect email address.

	• The document was not encrypted and the unintended recipient may have accessed the attached document containing the personal information of the client. • The Organization confirmed the incorrect email address has a valid user ID (as the employee sender did not receive a rejection notice). • The breach was discovered the same day.
Affected individuals	The incident affected 2 individuals.
Steps taken to reduce risk of harm to individuals	• Tried to recall the email. • Requested the unintended recipient to discard and not circulate the information and contact the Organization. • Changed investment account numbers. • Flagged the clients' account and put credit monitoring services in place. • Will no longer include detailed personal sensitive information, such as account numbers, when distributing client documents electronically. • Stressed with all employees that all client related materials sent electronically must be encrypted and password protected. • Conducted an internal review of employee procedures to ensure compliance with company policies, with a focus on remote working environments. • Held a special meeting with all staff to review this event and to reinforce all privacy procedures.
Steps taken to notify individuals of the incident	The affected individuals were notified verbally on May 15, 2020.
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 the possible harms that may occur as a result of the breach are "Identity theft, financial loss, negative effects on their credit record." I accept the Organization's assessment. A reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.

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 the likelihood of harm resulting from this incident is "Low, given the following factors: 1) the information was exposed to a sole unintended email recipient, 2) the unintended email recipient may be a dormant account, 3) the unitended [sic] email recipient may not have malicious intent, 4) the risk mitigation steps taken below." In my view, a reasonable person would consider that although the unauthorized disclosure was caused by human error and the email was accidently sent to a known unintended recipient, the likelihood of harm resulting from this incident is increased because the Organization could not recall the email and was not able to obtain confirmation from the unintended recipient that the email was deleted and not copied, forwarded or otherwise distributed. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, these safeguards do not necessarily mitigate the potential harm that may result if the information accessed were to be used for fraudulent purposes, for example.

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. A reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. Although the unauthorized disclosure was caused by human error and the email was accidently sent to a known unintended recipient, the likelihood of harm resulting from this incident is increased because the Organization could not recall the email and was not able to obtain confirmation from the unintended recipient that the email was deleted and not copied, forwarded or otherwise distributed. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, these safeguards do not necessarily mitigate the potential harm that may result if the information accessed were to be used for fraudulent purposes, for example. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individuals verbally on May 15, 2020 in accordance with the *Regulation*. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner