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	WealthBar Financial Services Inc. (Organization)
Decision number (file number)	P2018-ND-105 (File #009237)
Date notice received by OIPC	July 19, 2018
Date Organization last provided information	July 19, 2018
Date of decision	August 7, 2018
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 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 a portfolio manager that provides investment advisory services to Canadian clients through an online platform, and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information about the Organization's clients and prospects was downloaded by an unauthorized party: • first and last name, • email address, • residential address (if provided by the client or prospect), • business address (if provided by the client or prospect), • responses to survey questions (but without the survey questions to which the responses related). This information is about identifiable individuals 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 engaged an online survey service provider based in Barcelona, Spain, Typeform, to distribute surveys to clients and prospects. Typeform gathered survey responses and provided them to the Organization for integration into the Organization's own systems. Typeform maintained copies of survey responses on its cloud-based servers. • On June 29, 2018, Typeform advised the Organization that an unknown third party gained access to its back-up systems and downloaded certain information collected from the Organization's clients and prospects, from surveys provided by Typeform, on behalf of the Organization. • Typeform advised the Organization that the incident was identified on June 27, 2018 at 2 PM CET, and that by 2:30 PM CET, actions had been taken to remedy the cause of the incident that enabled the unknown third party to gain access to Typeform's systems.
Affected individuals	The incident affected 65 of the Organization's clients or prospects resident in Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted a comprehensive investigation. • Terminated the engagement with Typeform and took steps to delete the Organization's data from Typeform's platform. • Monitoring the Organization's systems.
Steps taken to notify individuals of the incident	The Organization reported that it "…notified affected individuals in Canada, including affected individuals in the Province of Alberta" and provided a copy of the notification to my office.
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 personal information involved in this incident is non-sensitive in nature, essentially "phone-book" information and …responses to survey questions that were either non-sensitive or otherwise rendered effectively meaningless (since they appeared without the survey questions). As such, [the Organization] maintains that the actual information that was accessed does not pose a real risk of significant harm to the affected individuals." The Organization provided a screenshot to demonstrate how response information from the surveys appeared in information downloaded by the unauthorized third party from Typeform's system. The Organization said that "the responses are very difficult to understand and in most cases are effectively meaningless". The Organization's notice to affected individuals said "At the moment, there is no indication of any access or misuse of your

	personal information. We always recommend that you remain vigilant in your awareness of potential email phishing schemes and beware of suspicious emails." I agree with the Organization that the survey response information, without the context of the survey questions, could be difficult for an average person to understand, although it seems possible that a sophisticated attacker with technological skills could likely make use of the information: the information as presented is in clear text. In any event, email addresses are clear and combined with other contact information and mere association with the Organization could be used for phishing purposes. I have previously said a reasonable person would consider phishing to be a significant harm.
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 noted that it "has not received any client complaints, and there has been no evidence of any subsequent misuse of the personal information in question." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to deliberate malicious action (cyber-attack). The Organization reported that Typeform worked quickly to remedy the situation after discovering the incident; however, the Organization did not report how long the information was exposed. In any event, it was long enough that it was downloaded by the unauthorized third party and is therefore available to be used by the perpetrators. The fact that there have been no reports of the information being misused to date, does not mitigate the risk that the information could be misused in the future.

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. The survey response information, without the context of the survey questions, could be difficult for an average person to understand, although it seems possible that a sophisticated attacker with technological skills could likely make use of the information: the information as presented is in clear text. In any event, email addresses are clear and combined with other contact information and mere association with the Organization could be used for phishing purposes. I have previously said a reasonable person would consider phishing to be a significant harm.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to deliberate malicious action (cyber-attack). The Organization reported that Typeform worked quickly to remedy the situation after discovering the incident; however, the Organization did not report how long the information was exposed. In any event, it was long enough that it was downloaded by the unauthorized third party and is therefore available to be used by the perpetrators. The fact that there have been no reports of the information being misused to date, does not mitigate the risk that the information could be misused in the future.

I require the Organization to notify the affected individuals whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that the Organization notified affected individuals in Alberta in accordance with the Regulation. The Organization is not required to notify the affected individuals in Alberta again.

Jill Clayton
Information and Privacy Commissioner