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	Collabria Financial Services Inc. (Organization)
Decision number (file number)	P2022-ND-082 (File #024066)
Date notice received by OIPC	June 3, 2022
Date Organization last provided information	June 10, 2022
Date of decision	January 10, 2023
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose personal 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 issuer of credit cards. 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, • address, • phone number, • email address, • date of birth, • social insurance number, • debt amount, and • accounts receivable information. 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 March 19, 2022, UPLevel, one of the Organization's suppliers providing debt collection services, suffered from an incident that compromised files containing their client database for a few hours. • Some files on UPLevel's network were copied and accessed without authorization. • On April 26, UPLevel notified the Organization of a malware incident and informed the Organization that some of the compromised files might be files from the Organization's card holders. • On May 11, UPLevel sent the Organization data which enabled it to confirm that the personal information of clients was potentially compromised by this incident. • The Organization's systems were never compromised.
Affected individuals	The incident affected 731 individuals.
Steps taken to reduce risk of harm to individuals	<u>UPLevel:</u> • Shutdown its systems. <u>Organization:</u> • Offered complimentary 5-year credit monitoring service. • Reissuing credit cards on a risk-based assessment to cardholder or upon request.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on June 24, 2022.
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 are "Identity theft, credit card fraud." I agree with the Organization's assessment. A reasonable person would consider the contact, identity and financial information potentially at risk could be used to cause the significant harms of identity theft, and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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	The Organization reported, *There is a high risk that the personal information [sic] be used with ill-intent.* I agree with the Organization's assessment. A reasonable person would consider that the likelihood of harm resulting from this

between the incident and the possible harm.	incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion and installation of malware). As well, the Organization reported that some files on UPLevel's network were copied and accessed without authorization.

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.

Contact, identity and financial information potentially at risk could be used to cause the significant harms of identity theft, and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion and installation of malware). As well, the Organization reported that some files on UPLevel's network were copied and accessed without authorization.

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

I understand the Organization notified affected individuals by letter on June 24, 2022, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance