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	Nissan Canada Finance (Organization)
Decision number (file number)	P2022-ND-021 (File #022275)
Date notice received by OIPC	April 8, 2021
Date Organization last provided information	April 8, 2021
Date of decision	April 22, 2022
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 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 "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, and • email address. 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. The Organization reported, "*There is no evidence at this time that this incident involved any financial or payment card information or customer login/password information*."
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about February 4, 2021, a perpetrator unlawfully accessed an Amazon Web Services (AWS) server on three separate instances using two different IP addresses. • The perpetrator exploited a vulnerability on one of Organization's AWS servers and, upon searching the

	compromised server, was able to obtain a single salesforce system ID. • This ID was of limited scope and the perpetrator used it access the recent "activity view" of interactions of that specific ID on February 6, 2021. • The Organization reported that it does not believe any information was actually downloaded from Salesforce system on February 6, 2021 because (i) the perpetrators had access to the user interface view, which did not permit the downloading of any information (and therefore any perpetrator would have been limited to taking screenshots or manually writing down information in order to exfiltrate it), and (ii) if any information had been downloaded from the salesforce system, salesforce system logs would have logged a V-flag indicator, and no such indicator appears to have been logged.
Affected individuals	The incident affected 1337 individuals.
Steps taken to reduce risk of harm to individuals	• Secured the affected system. • Notified Canadian privacy regulators.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on April 6, 2021.
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.	In its letter to my Office, the Organization did not assess the possible harms that may occur as a result of the incident. However, the notification to affected individuals stated: *It is always a good idea to scrutinize emails closely to avoid becoming a victim of an email scam. You may get an email that looks like it's from a real company or the Government of Canada. It may ask you for private information, such as your date of birth, passwords or credit card details. Sometimes the email will tell you to visit a fake website. If you get this kind of email, don't click on any links or give any information about yourself. If you have any doubts about where the email came from, make sure to check the identity of the sender.* In my view, a reasonable person would consider that the contact information along with email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.
Real Risk The likelihood that the significant harm will result must	The notification to affected individuals stated: *We are not aware of any reports of identity theft or other fraud*

be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	*related to this incident.* In its letter to my Office, the Organization stated: *NCF believes the risk to affected consumers to be extremely small. Nonetheless, NCF has notified each of the potentially affected persons via email.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach. Finally, the information may have been exposed for two (2) days.

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 information along with email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach. Finally, the information may have been exposed for two (2) days.

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 the Organization notified affected individuals by email on April 6, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner