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	Citrix Systems Canada Inc. (Organization)
Decision number (file number)	P2019-ND-198 (File #013162)
Date notice received by OIPC	April 30, 2019
Date Organization last provided information	April 30, 2019
Date of decision	December 16, 2019
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 Organization reported that it "…determined that the removed files contained information about our current and former employees, and, in limited cases, information about beneficiaries and/or dependents. This information may have included, for example, names, national ID numbers, and financial information". 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	• On March 6, 2019, the FBI informed the Organization that the FBI had reason to believe that international cyber criminals gained access to the Organization's internal network. • The Organization believes that the cyber criminals had intermittent network access between October 13, 2018 and March 8, 2019, and that they removed files from the Organization's internal systems during that time period.

Affected individuals	The incident affected approximately 40 current or former employees who are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Engaged cyber security firm to assist with forensic investigation. • Cooperating with the FBI. • Took measures to remove the cyber criminals' access, including a system wide password reset, tightened the rules related to password complexity and enhanced multifactor authentication. • Actively monitoring for signs of further activity or compromise. • Offered complimentary credit monitoring services to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter beginning April 29, 2019.
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 did not specifically identify potential harm(s) that might result from this incident, but its notice to affected individuals said "You should remain vigilant, including by regularly reviewing your financial account statements and monitoring free credit reports, if available in your jurisdiction. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions". In my view, a reasonable person would consider that the identity and financial information at issue could be used to cause the significant harms of identity theft and fraud.
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 did not specifically assess the likelihood of harm resulting from this incident. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action) over approximately 5 months and the Organization reported the attackers "…removed files from the Organization's internal systems during that time period".
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 identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action) over approximately 5 months and the Organization reported the attackers "…removed files from the Organization's internal systems during that time period".

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

I understand individuals were notified by letter beginning April 29, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner