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	US Fertility LLC and Shady Grove Fertility (Organizations)
Decision number (file number)	P2021-ND-272 (File #020869)
Date notice received by OIPC	May 10, 2021
Date Organization last provided information	May 10, 2021
Date of decision	February 14, 2022
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organizations are 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"	US Fertility LLC is a company providing IT platforms and management services to a number of fertility clinics in the United States, including Shady Grove Fertility. These organizations offer services to Canadians who travel to the US for the purposes of receiving fertility treatments. The Organizations are "organizations" 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: • first and last name, • address (in some instances only partial address information), • email address, • date of birth, • personal health information (e.g. an internal patient identifier, name of healthcare provider, diagnostic information), and • passport 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 September 14, 2020, the Organizations discovered that a third party had gained unauthorized access to some computer systems. Data on some of the servers and workstations were encrypted by ransomware. • A forensic investigation confirmed that the unauthorized actor acquired a limited number of files during the period of unauthorized access, which occurred between August 12, 2020 and September 14, 2020. • The Organizations reported there is no evidence of actual misuse of personal information as a result of the incident.
Affected individuals	The incident affected 883,989 individuals, including 122 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Removed systems from the network. • Remediated the malware and ensured the security of the environment. • Fortified firewall security. • Performed a comprehensive review to identify individuals whose personal information may have been involved. • Notified federal law enforcement authorities in the United States of the incident and cooperated with their investigation. • Notified all potentially affected individuals about the incident, and shared best practices for responding to such incidents. • Set up a dedicated call centre to assist affected individuals. • Offered a credit-monitoring product for 12 months to potentially affected individuals. • Adapted employee training protocols relating to data protection and security, including training targeted at recognizing phishing emails.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on April 12, 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.	The Organization reported, *The possible consequences might include the loss of confidentiality of personal information including personal health information, along with an increase in vulnerability to phishing or other social engineering attacks.* In my view, a reasonable person would consider the contact, identity and medical information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Medical information could also be used to cause hurt, humiliation and embarrassment. 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 between the incident and the possible harm.	The Organization reported, *While there is no indication that the personal information affected by the incident was or will be misused, there is a possibility that the harm … could materialize, given the nature of the incident.* 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, ransom demand). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. The information was exposed for approximately 1 month.

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 the contact, identity and medical information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Medical information could also be used to cause hurt, humiliation and embarrassment. 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 an unknown third party (deliberate intrusion, ransom demand). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. The information was exposed for approximately 1 month.

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 the Organization notified affected individuals by mail on April 12, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner