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	NUUD Inc. o/a HUSH Lingerie and More (Organization)
Decision number (file number)	P2021-ND-179 (File #0019891)
Date notice received by OIPC	November 26, 2020
Date Organization last provided information	November 26, 2020
Date of decision	September 2, 2021
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 operates in Alberta and 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 about customers: • name, • telephone number, 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 this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On February 5, 2019, the Organization was informed by another franchise owner that individuals from the corporate store entered the Organization's location saying they were there to update the Organization's point of sale system. • The Organization believed these actions to be suspicious as the corporate office did not provide IT support previously.

	• On February 8, 2019, the Organization discovered spyware (called "Spyrix") installed on its computer remotely. • On February 14, 2019, the Organization contacted the corporate office, and the corporate office said it removed the software but wanted to reinstall it. • The Organization reported that shortly after receiving OIPC breach notification Decision P2020-ND-120 (related to this matter), the Organization discovered "an entire database of customers" that may be at risk. • The Organization reported "our systems (point of sale systems) are cloud base [sic] and all connected which is why i [sic] have reason to believe all of the information tied to the systems were or are at risk."
Affected individuals	The Organization reported the number of affected individuals is "unknown".
Steps taken to reduce risk of harm to individuals	The Organization did not identify steps taken to reduce the risk of harm to affected individuals.
Steps taken to notify individuals of the incident	The Organization reported "No clients in the customer database have been notified."
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 harms that may occur as a result of the breach. In its report of the breach, the Organization said: *From client database - personal information, telephone numbers, email addresses.* In my view, a reasonable person would consider that the contact information at issue, including email address and association with the Organization as a client, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are 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.	In assessing the likelihood that significant harm will result from this breach, the Organization said "It is unclear at this time". 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 a deliberate intrusion into the Organization's computer system, for an unknown purpose. Further, the information may have been exposed for approximately two weeks.

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 at issue, including email address and association with the Organization as a client, could be used for the purposes of phishing, increasing the affected individuals' 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 a deliberate intrusion into the Organization's computer system for an unknown purpose. Further, the information may have been exposed for approximately two weeks. **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), and confirm to my office in writing, within 10 days of the date of this decision, that this has been done.**

Jill Clayton
Information and Privacy Commissioner