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	Felix Pharmacy West Inc. (Organization)
Decision number (file number)	P2023-ND-001 (File #027687)
Date notice received by OIPC	October 11, 2022
Date Organization last provided information	October 26, 2022
Date of decision	February 1, 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 a licensed pharmacy located in Coquitlam, B.C. 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, • phone number, • postal address, • date of birth, • sex, • prescription information, • insurance plan number, and • other patient notes (e.g., allergies, diagnoses, refill requirements, reason for contacting the pharmacy, etc.). • In certain instances, health card numbers were also contained on the encrypted server. 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 16, 2022, the Organization became aware of an IT issue impacting its local operations. Specifically, Felix West employees were unable to access the local pharmacy database server. • The Organization discovered that an unauthorized third party initially gained access to the pharmacy's systems on May 29, 2022 and encrypted certain servers on September 16, 2022. • The Organization reported, "*there is no evidence of any actual access to or exfiltration of customer personal information, however, Felix West cannot rule out the possibility that this occurred.*"
Affected individuals	The incident affected 4295 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Took steps to steps to secure network. • Engaged external cybersecurity experts to assist in the containment, remediation, forensic investigation and business restoration efforts. • Engaged legal counsel. • Purchased new systems and generated a new network. • Introducing new company-wide policies related to security and privacy, and engaging IT professionals to ensure secure setup and long-term network security. • Notified the College of Pharmacists of British Columbia. • Offered a two-year credit monitoring solution.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent by email and/or notified by postal mail from October 12, 2022 to October 28, 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 *Although Felix West believes that there is a low likelihood that harm will result from this incident, there may be a risk of embarrassment to individuals whose records contain sensitive prescription information.* In my view, a reasonable person would consider the contact, identity, and insurance plan number could be used to cause the significant harms of identity theft and fraud. The medical and prescription information could 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: *Given the lack of evidence of any actual access to, exfiltration of or misuse of customer personal information, and the steps that Felix West took to reduce the risk of harm (including notification to affected individuals…), Felix West believes that there is a low likelihood that harm will result from this incident.* The organization also reported: *There is no evidence of any actual access to or exfiltration of customer personal information, however, Felix West cannot rule out the possibility that this occurred.* 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 the malicious action of an unknown third party (deliberate intrusion, encryption). Although the Organization has put additional safeguards, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's systems were to be used for fraudulent purposes. The lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach.

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 insurance plan number could be used to cause the significant harms of identity theft and fraud. The medical and prescription information could 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, encryption). Although the Organization has put additional safeguards, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's systems were to be used for fraudulent purposes. The lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident, as identity theft can happen months and even years after a data breach.

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 letter sent by email and/or postal mail from October 12, 2022 to October 28, 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