



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

| | |
|---|---|
| Organization providing notice under section 34.1 of PIPA | U.S. Fund for UNICEF (Organization) |
| Decision number (file number) | P2015-ND-80 (File #P2571) |
| Date notice received by OIPC | February 11, 2014 |
| Date Organization last provided information | July 14, 2014 |
| Date of decision | December 23, 2015 |
| Summary of decision | There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA or the Act). |
| JURISDICTION | |
| Section 1(1)(i) of PIPA “organization” | <p>The Organization is incorporated in New York State as a not-for-profit corporation.</p> <p>Section 56(3) limits the application of PIPA to personal information collected, used or disclosed by a “non-profit organization” in connection with a commercial activity. Although it operates on a not-for-profit basis, the Organization is not a “non-profit organization,” as defined by section 56(1)(b)(i) of PIPA.</p> <p>The Organization is an “organization” as defined in section 1(1)(i)(i) of PIPA and is fully subject to the Act.</p> |
| Section 1(1)(k) of PIPA “personal information” | <p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• telephone number,• credit card information, including security code and expiration date. |

| | |
|--|--|
| | This information is about an identifiable individual, and qualifies as “personal information” as defined in section 1(1)(k) of PIPA. The information was collected by telephone from a resident of Alberta. |
| DESCRIPTION OF INCIDENT | |
| <input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure | |
| Description of incident | <ul style="list-style-type: none"> • On or about December 2, 2013, the Organization discovered that an unauthorized individual or individuals gained access to one of its servers. • The Organization determined that a portion of the exposed information contained personal information. |
| Affected individuals | One (1) individual residing in Alberta. |
| Steps taken to reduce risk of harm to individuals | <ul style="list-style-type: none"> • Disconnected server immediately upon discovery of unauthorized access. • Hired forensic expert to assess extent of incident. • Notified affected individual. • Offered one year of credit monitoring services and identity restoration service to affected individuals. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta (OIPC). |
| Steps taken to notify individuals of the incident | Notification sent by mail on January 27, 2014. |
| 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. | <p>In its report to the OIPC, the Organization did not specifically assess the harm that could result from this incident. However, the notification sent to the affected individual provided information for protecting oneself from “possible identity theft or other financial loss”.</p> <p>In my view, the personal information involved is sensitive and could be used to cause the harms of identity theft, fraud and financial loss. These are significant harms.</p> |
| Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and | <p>In its report to the OIPC, the Organization did not specifically assess the likelihood of harm resulting from this incident. However, the notification sent to the affected individual advised of “an incident that may affect the security of your personal information,” although “we have no evidence to date of attempted or actual misuse of your information”.</p> |

| | |
|---|--|
| effect relationship between the incident and the possible harm. | In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessed intentionally by an unauthorized and unknown party. |
| DECISION UNDER SECTION 37.1(1) OF PIPA | |
| <p>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 individual. The personal information involved is sensitive and could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the personal information was accessed intentionally by an unauthorized and unknown party.</p> <p>I require the Organization to notify the affected individual in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization notified the affected individual by mail on January 27, 2014, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individual again.</p> | |

Jill Clayton
Information and Privacy Commissioner