



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

| | |
|--|---|
| Organization providing notice under section 34.1 of PIPA | Drillinginfo, Inc. (Enverus) (Organization) |
| Decision number (file number) | P2020-ND-146 (File #017797) |
| Date notice received by OIPC | October 20, 2020 |
| Date Organization last provided information | October 26, 2020 |
| Date of decision | November 17, 2020 |
| 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 whose personal information was collected in Alberta pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (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 incident involved all or some of the following information: <ul style="list-style-type: none">• pay statements, and• access to the Social Insurance Number reveal page. This information is about an identifiable individual and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies. |
| DESCRIPTION OF INCIDENT | |
| <input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure | |
| Description of incident | <ul style="list-style-type: none">• The Organization uses a service provider, ADP Canada, to manage its employees’ self-service accounts.• On September 28, 2020, an employee of the Organization reported that he received a notification that a mobile number change was made to his ADP profile, and a time-off request was entered that he did not make. |

| | |
|--|---|
| | <ul style="list-style-type: none"> ADP Canada advised the Organization that a technical issue with a password recovery process enhancement may have led to another ADP client’s employee inadvertently accessing personal information of the Organization’s employee. The breach ended on October 2, 2020. |
| Affected individuals | The incident affected one (1) Alberta resident. |
| Steps taken to reduce risk of harm to individuals | <p>The Organization:</p> <ul style="list-style-type: none"> Contacted ADP for assistance immediately. Changed credentials for all employees in Canada and the US. Initiated an investigation with key stakeholders. Reviewed logs and continue to monitor for anomalies. Made numerous attempts to collaborate with ADP. Currently exploring additional options that can be provided to the employee in this area. <p>ADP Canada:</p> <ul style="list-style-type: none"> Turned off the feature and reset passwords for the affected accounts. Conducted a log analysis to identify accounts where the password feature was used during the time period in question. Offered complimentary twelve (12) month membership to an internet surveillance/fraud remediation service. |
| Steps taken to notify individuals of the incident | The affected individual was notified verbally by the Organization and in writing by the service provider on October 22, 2020. |
| REAL RISK OF SIGNIFICANT HARM ANALYSIS | |
| <p>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> | <p>The Organization reported:</p> <p><i>Personal information can be used for many malicious things. In this case, it we understand it to have been revealed tp [sic] another ADP client’s employee inadvertently accessing our employees’ account. We believe this is a risk in and of itself to our employee.</i></p> <p>I accept the Organization’s assessment that a reasonable person would consider that the employment and identity information at issue could be used to cause the significant harms of identity theft and fraud.</p> |

| | |
|---|--|
| <p>Real Risk</p> <p>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.</p> | <p>The Organization reported:</p> <p><i>ADP Canada states in their memo they discovered a technical issue with the enhancement that may have led to another ADP client's employee inadvertently accessing your employees' account. Information was exposed to this party as we understand it today...</i></p> <p>In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is decreased as the breach resulted from human error and not malicious intent. However, the Organization did not provide any additional information concerning whether or not its employee's personal information was downloaded, copied or otherwise re-distributed by the other ADP client's employee. As well, the information may have been exposed for approximately one (1) week.</p> |
| <p>DECISION UNDER SECTION 37.1(1) OF PIPA</p> | |
| <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.</p> <p>I accept the Organization's assessment that a reasonable person would consider that the employment and identity 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 decreased as the breach resulted from human error and not malicious intent. However, the Organization did not provide any additional information concerning whether or not its employee's personal information was downloaded, copied or otherwise re-distributed by the other ADP client's employee. As well, the information may have been exposed for approximately one (1) week.</p> <p>I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the affected individual was notified verbally by the Organization and in writing by the service provider on October 22, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individual again.</p> | |

Jill Clayton
Information and Privacy Commissioner