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** | IQ Insurance Services, Inc. (Organization) |
| **Decision number (file number)** | P2019-ND-133 (File #012183) |
| **Date notice received by OIPC** | February 27, 2019 |
| **Date Organization last provided information** | February 27, 2019 |
| **Date of decision** | August 12, 2019 |
| **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 *Personal Information Protection Act* (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 the following information:<br><br>• first and last name,<br>• address,<br>• telephone number,<br>• email address,<br>• date of birth.<br><br>This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ❑ unauthorized access ☒ unauthorized disclosure | |
| **Description of incident** | On February 21, 2019, the information at issue was emailed to the wrong email address. The employee who sent the email discovered the error immediately after sending. |
| **Affected individuals** | The incident affected one individual. |

| | |
|---|---|
| **Steps taken to reduce risk of harm to individuals** | • Sent a follow-up email to the same (incorrect) email address to request the information be deleted. At the time of reporting, no response had been received.<br>• Sent test emails to the "wrong email" to determine if the address was valid. Tod date, the process has "proved inconclusive".<br>• Will now copy/paste email addresses to prevent reoccurrence. |
| **Steps taken to notify individuals of the incident** | The affected individual was notified by email on February 22, 2019. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>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 harm that might result from this incident was "Wrongful impersonation; potential may exist for identity theft".<br><br>In my view, a reasonable person would consider that the contact and identity information could be used to cause the harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. |
| **Real Risk**<br>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 the likelihood of harm resulting from this incident as "Low risk as most information is likely in the public domain." The Organization also said "We cannot verify that that [sic] the unintended email addressee is a valid or invalid gmail address. An we verify it is an invalid gmail address [sic]. It is not a certainty that the customer's information was actually received or read by an unintended third party, but a risk exists."<br><br>In my view, a reasonable person would consider that the likelihood of harm is decreased because the breach did not result from malicious intent, but rather human error. However, the Organization has been unable to confirm that the email address is valid/invalid, and has not been able to confirm that the personal information has been deleted and was not forwarded/used. |
| **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 individual. | |

A reasonable person would consider that the contact and identity information could be used to cause the harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm is decreased because the breach did not result from malicious intent, but rather human error. However, the Organization has been unable to confirm that the email address is valid/invalid, and has not been able to confirm that the personal information has been deleted and was not forwarded/used.

The Organization is required to notify the affected individual, in accordance with section 19.1 of the *Personal Information Protection Act Regulation*.

I understand the affected individual was notified by email on February 22, 2019. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner