



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

| | |
|--|--|
| Organization providing notice under section 34.1 of PIPA | World Financial Group Insurance Agency of Canada (Organization) |
| Decision number (file number) | P2021-ND-245 (File #020901) |
| Date notice received by OIPC | February 8, 2021 |
| Date Organization last provided information | November 11, 2021 |
| Date of decision | December 1, 2021 |
| 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). |
| 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” | <p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• date of birth,• social insurance number,• address,• account number, and• investment funds. <p>This information is about an identifiable individual and is “personal information” as defined in section 1(1)(k) of PIPA.</p> |
| 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">• On January 28, 2021, an agent's assistant sent emails containing a partially completed trade ticket to a client for his review and signature.• The client notified the agent that no email was received.• On January 29, 2021, the agent's assistant resent the emails. |

| | |
|--|---|
| | <ul style="list-style-type: none"> • Again, the client confirmed that no email was received. • The agent check his assistant's outbox and noticed that the email address for the client was incorrect. |
| Affected individuals | The incident affected 1 individual. |
| Steps taken to reduce risk of harm to individuals | <ul style="list-style-type: none"> • Escalated the incident to the Organization’s Privacy Officer. • Notified the client of the situation and is currently redeeming the affected account as a precaution. • Advised the client to get identity monitoring for a year as additional security measures. • Working with staff and advisors to remind them of the importance of being diligent in checking that email address are correct before sending out emails which contain sensitive information. • Suggested including password protected files and sending the password to the intended recipient via a different form of communication. |
| Steps taken to notify individuals of the incident | The affected individual was notified by letter on February 26, 2021. |
| 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 the possible harms that might result from this incident include:</p> <ul style="list-style-type: none"> -<i>Identity Fraud</i> -<i>Account Take Over</i> -<i>Funds Re-Directed to a third party</i> <p>I agree with the Organization’s assessment. A reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft and/or fraudulent transactions.</p> |
| <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 effect relationship between the incident and the possible harm.</p> | <p>The Organization reported:</p> <p style="text-align: center;"><i>There is medium risk that harm could result from this breach. The unintended recipient could access the client's account using the information he received in the email.</i></p> <p>In my view, a reasonable person would consider that the likelihood of harm is reduced because the incident was caused by human error and the email was accidentally sent to a known unintended recipient. However, the Organization reported “The agent had made 3 attempts to contact the unintended recipient to ask that</p> |

| | |
|--|---|
| | they delete the email that they received in error, however no response was received.” |
| 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.</p> <p>A reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft and/or fraudulent transactions. The likelihood of harm is reduced because the incident was caused by human error and the email was accidentally sent to a known unintended recipient. However, the Organization reported “The agent had made 3 attempts to contact the unintended recipient to ask that they delete the email that they received in error, however no response was received.”</p> <p>I require the Organization to notify the affected individual in accordance with section 19.1 of the Personal Information Protection Act Regulation (Regulation).</p> <p>I understand the Organization notified the affected individual by letter on February 26, 2021, in accordance to the Regulation. The Organization is not required to notify the affected individual again.</p> | |

Jill Clayton
Information and Privacy Commissioner