



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

| | |
|--|--|
| Organization providing notice under section 34.1 of PIPA | BSH Home Appliances (Organization) |
| Decision number (file number) | P2021-ND-261 (File #020920) |
| Date notice received by OIPC | February 11, 2021 |
| Date Organization last provided information | November 13, 2021 |
| Date of decision | February 8, 2022 |
| Summary of decision | There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify affected individuals 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 operates a call center for its brands that customers can use to request parts, make warranty claims or ask for technical assistance. 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">• first and last name,• street address (city, province, postal code, country), and• credit card information (including card number, expiration date and CVV Code). This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies. |
| DESCRIPTION OF INCIDENT | |
| <input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure | |

| | |
|--|---|
| <p>Description of incident</p> | <ul style="list-style-type: none"> • In early December 2020, the Organization investigated several customer complaints regarding unauthorized credit card transactions. • The Organization discovered that a temporary employee in the United States had been improperly requesting credit card information from callers and using that information to make unauthorized purchases. • The Organization promptly terminated the employee as such collection and use was not authorized and contrary to the Organization’s policies. |
| <p>Affected individuals</p> | <p>The incident affected four (4) individuals, including one (1) Alberta resident.</p> |
| <p>Steps taken to reduce risk of harm to individuals</p> | <ul style="list-style-type: none"> • Offered one year free credit-monitoring service, and provided information as to how to mitigate the risk. • Terminated the temporary employee suspected of collecting and misusing the credit card information. • Notified the Competition Bureau and local authorities about the incident. • Intends to implement further training and screening procedures to ensure that call center employees are not collecting any customer information unless required for a transaction. |
| <p>Steps taken to notify individuals of the incident</p> | <p>The affected individual was notified by letter on February 10, 2021.</p> |
| <p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p> | |
| <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 style="text-align: center;"><i>There is the possibility of unauthorized credit card use, however [the Organization] has no indication that any misuse has occurred in the case of the Canadian customer who contacted the Call Centre.</i></p> <p>In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft, fraud and/or financial loss. These are all significant harms.</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>To date, it does not appear that any misuse has been made of the Canadian caller's credit card information, if this was indeed misappropriated.</i></p> <p>In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because it resulted from deliberate and malicious actions (unauthorized access and theft) by a rogue employee. The lack of reported incidents resulting from this breach to date is not a mitigating factor as identity theft, fraud and/or financial loss can occur months and even years after a data breach.</p> |
|---|---|

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.

A reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft, fraud and/or financial loss. These are all significant harms.

The likelihood of harm resulting from this incident is increased because it resulted from deliberate and malicious actions (unauthorized access and theft) by a rogue employee. The lack of reported incidents resulting from this breach to date is not a mitigating factor as identity theft, fraud and/or financial loss can occur months and even years after a data breach.

I require the Organization to notify the affected individual whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that affected individual was notified by letter on February 10, 2021. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner