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** | EyeBuyDirect, Inc. (Organization) |
| **Decision number (file number)** | P2017-ND-18 (File #002022) |
| **Date notice received by OIPC** | November 20, 2015 |
| **Date Organization last provided information** | November 20, 2015 |
| **Date of decision** | January 30, 2017 |
| **Summary of decision** | There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals 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)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | Some or all of the following information was involved in this incident:<br><br>• name (first, middle, last),<br>• mailing address,<br>• shipping address,<br>• telephone number,<br>• email address,<br>• credit card number, and<br>• credit card security code.<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's e-commerce website. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss | ☒ unauthorized access ❑ unauthorized disclosure |

| | |
|---|---|
| **Description of incident** | • On June 16, 2015, the Organization learned that hackers using a Russian IP address gained unauthorized access to the Organization's website.<br>• The Organization's website was accessed between February 9 and May 30, 2015. During this time, the unauthorized individual(s) may have accessed the information at issue. |
| **Affected individuals** | The incident affected 24 residents of Alberta. |
| **Steps taken to reduce risk of harm to individuals** | • Retained forensic investigators to assess the incident.<br>• Implemented additional security measures to reduce the likelihood of reoccurrence.<br>• Offered no-cost identity protection service to affected individuals. |
| **Steps taken to notify individuals of the incident** | Written notice of the incident was mailed to affected residents of Alberta during the week of October 19, 2015. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>Some damage or detriment or injury that could be caused to the 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. | In its report of the breach, the Organization did not specifically identify any potential harm that might result to affected individuals from the incident. However, the Organization did advise potentially affected individuals that "with incidents involving fraud or identity theft, it is important to be informed." Further, the Organization offered identity theft protection to affected individuals.<br><br>In my view, the information at issue could be used to cause the harms of identity theft and fraud. In addition, email addresses could be used to cause the harm of phishing. These are significant harms. |
| **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 did not assess the likelihood of harm resulting from this incident.<br><br>In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) and the information was exposed for approximately 3 ½ months. |
| **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 as a result of this incident. The information at issue could be used to cause the harms of identity theft and fraud. In addition, email addresses could be used to cause the harm of phishing. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) and the information was exposed for approximately 3 ½ months.<br><br>I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). | |

I understand that written notice of the incident, in accordance with the Regulation, was mailed to affected residents of Alberta during the week of October 19, 2015. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner