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	eBay Inc. (the Organization)
Decision number (file number)	P2015-ND-56 (File #2744)
Date notice received by OIPC	May 21, 2014
Date Organization last provided information	June 4, 2014
Date of decision	August 27, 2015
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 a "global marketplace". I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA and the information at issue was collected in Alberta.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • customer name, • encrypted password, • email address, • physical address, • telephone number, and • date of birth. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• In early May 2014, the Organization detected a sophisticated cyberattack which compromised a database containing encrypted passwords and other non-financial data. • The database was compromised between late February 2014 and early March 2014. • The Organization's systems detected the remote access compromise. The affected database was located in the US.
Affected individuals	The Organization did not provide an estimate of the number of affected individuals, instead reporting that it has a total of 11.4 million active and inactive accounts in Canada. The Organization does not break these numbers down by Canadian province. This number does not represent the number of user accounts (which, the Organization reports, would be lower).
Steps taken to reduce risk of harm to individuals	• Worked with law enforcement and leading security experts to investigate the incident. • Took steps to identify the level of access to systems and data, contain the illegal access and prevent further access. • Disabled customer passwords and encouraged customers to change their passwords on the Organization's site and any other sites where they may have used the same password. • Notified international and national data protection authorities.
Steps taken to notify individuals of the incident	The Organization notified affected individuals by email sent in May 2014.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
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.	The Organization reported that it had no evidence that any customer financial or credit information was compromised and the "file did not contain any social security taxpayer identification or national identification information." In my view, despite the fact financial and credit information was not compromised in this incident, there remains a risk of identity theft and fraud because date of birth was involved. Further, customer email addresses were compromised and could be used to cause the harm of phishing risk. These are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere	The Organization reported that there is no evidence that the incident affected accounts for PayPal users, and no evidence of any unauthorized access to personal, financial or credit card information which is stored separately. The Organization did

speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	not include active URLs or links in its email notification to users to reduce the likelihood of harm resulting from phishing, and also implemented mechanisms for customers to verify that emails they received were from the Organization. In my view, the Organization reduced the risk of phishing harm resulting from this incident by taking these actions. However, because date of birth was compromised, and considering the number of affected individuals, malicious intent behind the cyberattack, and possibility that phishing attacks could occur well-after the incident itself, I consider the risk of harm resulting from this incident has not been fully mitigated.

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 resulting from this incident. Date of birth and customer email addresses were compromised and could be used to cause the significant harms of identity theft and phishing. Although the Organization took steps to reduce the risk of harm from phishing, considering the number of affected individuals, malicious intent behind the cyberattack, and possibility that phishing attacks could occur well-after the incident itself, I consider the risk of harm resulting from this incident has not been fully mitigated.

I require the Organization to notify affected Albertans in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the Regulation). As the Organization has already notified all affected individuals by email sent in May 2014, the Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner