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	Columbia Bank (Organization)
Decision number (file number)	P2019-ND-031 (File #006777)
Date notice received by OIPC	October 10, 2017
Date Organization last provided information	December 5, 2017
Date of decision	February 19, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individual whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is incorporated and operating in Washington State, USA, and 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: For one Alberta resident: • name. • Social Security Number (Alberta resident is US citizen). For other affected individuals - the above information, plus: • driver license number, • bank account number, and • payment card number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On July 25, 2017, the Organization learned that an unauthorized individual gained access to an employee's email account after the employee clicked on a link in a phishing email. • The unauthorized individual gained access to the employee's email on July 20, 2017. • The incident was discovered when phishing emails were sent from the employee's account.
Affected individuals	The incident affected one (1) individual residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to the US Federal Bureau of Investigation. • Worked with a forensic firm to initially disable and then secure the employee's email account. • Offered one-year free membership in credit monitoring and identity theft protection services to the affected individuals. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta.
Steps taken to notify individuals of the incident	The affected individual was notified by mail on October 6, 2017.
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 "Individuals affected by this incident are at a risk of harm through financial loss, fraud, identity theft and potential negative effects on a credit report." I agree with the Organization's assessment. A reasonable person would consider that the identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, financial loss and negative effects on a credit report.
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.	The Organization reported that it "…has no indication that any personal information was copied or misused in any way" and noted that it is "…offering a complimentary one-year membership in credit monitoring and identity theft protection services that will help individuals identify potential misuse of their personal information and provide immediate identification and resolution of fraud and identity theft". The Organization "…is also reminding the potentially affected individuals to remain vigilant to fraud and identity theft by reviewing their account statements and free credit reports." In my view, the likelihood of harm resulting from this incident is increased because the personal information was exposed as the result of a phishing incident, indicating malicious intent.

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 identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, financial loss and negative effects on a credit report. The likelihood of harm resulting from this incident is increased because the personal information was exposed as the result of a phishing incident, indicating malicious intent. 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 the Organization notified the affected individual in a letter dated October 6, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner