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	Connect Logistics Services Inc., and its affiliates, including DHL Global Forwarding (Canada) Inc., which are subsidiaries of Deutsche Post AG (Organization)
Decision number (file number)	P2020-ND-135 (File #014821)
Date notice received by OIPC	January 23, 2020
Date Organization last provided information	January 23, 2020
Date of decision	November 3, 2020
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 individuals 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 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: • name, • Social Insurance number, • date of birth, and • banking information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On December 11, 2019 an intruder compromised an employee's ADP (payroll system) account. The intrusion arose from a phishing attack.

	• The intruder accessed the ADP system for over 3 hours from December 11-13, 2019. • The intruder created fake employee profiles with real bank accounts in the United States. • The ADP system flagged the US bank accounts on December 13, 2019. Upon flagging, ADP immediately shut down access to the system, isolated the fraudulent accounts and engaged the Organization's IT professionals.
Affected individuals	The incident affected 4,600 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Provided current and former employees the opportunity to enroll in a one year credit monitoring service. • Required a password reset for all affected employees and will do so regularly going forward, along with additional IT security training and additional IT security measures to be determined.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and letter beginning the week of January 13, 2020.
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 did not specifically identify the possible harm(s) that might result from the incident, but did offer credit monitoring to affected individuals. Further, the Organization's notice to affected individuals advised "If you have an online ADP account please change your password as soon as possible … If you use the same password on banking or other websites we recommend you complete a password change as soon as possible." In my view, a reasonable person would consider that the identity and financial information at issue could be used to cause the significant harms of identity theft and fraud.
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 "Records indicate that the intruder did not run any reports or download employee information, however the intruder did have access to this information and could have taken screenshots, notes, or otherwise have recorded personal information." The Organization also said "At this time we are unable to determine a likelihood of harm that will result." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the breach was the result of malicious intent (deliberate intrusion and creation of fake employee profiles). The Organization cannot confirm the intruder did not take screenshots, notes or otherwise record the personal information.

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 and fraud. The likelihood of harm resulting from this incident is increased because the breach was the result of malicious intent (deliberate intrusion and creation of fake employee profiles). The Organization cannot confirm the intruder did not take screenshots, notes or otherwise record the personal information. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the affected individuals were notified by email and letter beginning the week of January 13, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner