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	Uber B.V. (Organization)
Decision number (file number)	P2018-ND-030 (File #007458)
Date notice received by OIPC	Uber Canada Inc., an affiliate of the Organization, initially contacted my office about this incident on November 23, 2017, and provided a copy of a notification form the Organization had submitted to the Dutch Data Protection Authority (DPA) on November 21, 2017. On November 25, 2017, Uber Canada Inc. confirmed to my office that the notification form "should not be considered a notification under section 34.1 of Alberta's *Personal Information Protection Act* because we do not believe the events at issue represent a real risk of significant harm to an individual as defined in the Act." On November 28, 2017, I initiated an investigation into this matter on my own motion, under section 36(1)(a) of PIPA. On January 8, 2018, and January 12, 2018, the Organization provided additional information about the incident to my office in response to the investigation. On February 26, 2018, Uber Canada Inc. confirmed Uber B.V. was the organization having control of the personal information at issue.
Date Organization last provided information	February 26, 2018
Date of decision	February 28, 2018
Summary of decision	Section 34.1(1) of PIPA states "An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information <u>where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.</u>" [my emphasis] Based on information provided to my office by the Organization via Uber Canada Inc., I determined that it was necessary to issue a Breach Notification Decision. On February 26, 2018, my office telephoned Uber Canada Inc. to provide notice of my finding that a reasonable person would consider that there exists a real risk of significant harm to individuals as a result of the unauthorized access to personal information in this case, thereby triggering the

	Organization's duty to provide notice to me under section 34.1(1). As a result of my finding and the urgency of notifying affected individuals under section 37.1(1) of PIPA, my office also informed Uber Canada Inc. that I would immediately be issuing this breach notification decision, prior to concluding the investigation into other matters of compliance with PIPA. Pursuant to section 37.1 (1) of PIPA, "Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure…". As I have decided that a reasonable person would consider that there exists a real risk of significant harm to the individuals affected by this incident, I require the Organization to notify those 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"	Uber Canada Inc. said that "Uber B.V., the Dutch entity that acts as the data controller for riders and drivers with Uber outside the United States, including those in Alberta, has provided information in response to questions posed in your December 20 email. Uber's Canada-based entity, Uber Canada Inc., is an affiliate of Uber B.V.". The Organization is an "organization" as defined in section 1(1)(i) of PIPA and collects personal information in Alberta.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information about the Organization's "users". The Organization identifies both riders and drivers as "users". • first and last name, • mobile telephone number/last confirmed mobile telephone number, • nickname, • receipt, • receipt email address, • email address, • hashed and salted password, • password changes, • user ID, • unique identifier (UUID), • user token,

	• mobile token, • email token, • location of sign-up, • sign-up “shape”, • location, • inviter ID, • inviter UUID, • recent fare splitter ID, • recent fare splitter UUID, • notes, • user rating, • boolean value, • promotions received or used, • banned flag (indicating whether user was banned), • fraud score, and • Clientinfo Authnet (includes internal identification information, links rider to payment profile stored with external payment provider). <u>Driver specific information</u> • driver ID, • driver’s license number, • driver rating, • professionalism score, • city knowledge score, • notes, and • payment statements (including how much drivers were paid, service fee rate, driver payout amount, Organization payout amount, trip request times, type of ride, driver’s UUID and time invoice created). This information is about identifiable individuals (drivers and riders), and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected from individuals through the Organization’s mobile application, website, or in-person driver support centres. To the extent these transactions occurred in Alberta, I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On November 14, 2016, "Uber was contacted by an individual who claimed he had accessed Uber user information." • The DPA report stated that "Uber investigated and determined that the individual and the other person working with him had obtained access to a private Uber developer page…. Using credentials located there, the unauthorized actor was able to access and download certain archived driver and rider data stored in a cloud-based server. The incident did not breach any corporate systems or infrastructure." • The DPA report stated that "To the best of Uber's knowledge, the unauthorized actor's access to this data began in October 13, 2016, and there was no further access by the actor to Uber's data after November 15, 2016." • The Organization said that "Uber's security team took immediate steps to respond to and limit the impact of the incident, including engaging in immediate and then ongoing communications with the original unauthorized actor and the second individual subsequently identified to have been working with him. Uber also determined the means of access, shut down the credential that had been used to gain entry…and took steps intended to confirm that the actors had destroyed and would not use or further disseminate the information…. identified the third parties, and met with them in person." • The Organization said "Uber's security team paid the outside actors to destroy the data, as demanded… and obtained assurances from the individuals that they had destroyed and would not use or further disseminate the downloaded information, and to the best of Uber's knowledge, such materials were destroyed."
Affected individuals	The incident affected approximately 32 million non-US riders. The Organization estimates there were 815,000 Canadians affected by the incident. The Organization said "the information Uber collects about users does not able the company to determine which users reside in Alberta in a manner that would be complete or definitive." The Organization said twenty-three (23) drivers "with an apparent connection to Canada" were affected by the breach, including one (1) driver with an Alberta address.
Steps taken to reduce risk of harm to individuals	• Determined the means of access and shut down the compromised credentials. • Engaged immediately and in ongoing communications with the unauthorized third party and a second individual.

	• Took steps to confirm that the third party destroyed and would not use or further disseminate the information. • Implemented additional measures to improve security posture, including additional access controls for services used by engineers. • Starting in October 2017, Uber hired a cyber security forensic company to analyze the data that was downloaded. • Offered drivers identity theft protection.
Steps taken to notify individuals of the incident	On January 8, 2018, the Organization said "…Uber has provided individual notice to all drivers globally, including the 23 drivers with an apparent connection to Canada….". Affected riders have not been notified of the incident.
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 assessed that "the information at issue was not sensitive and not the type that poses a threat of potential harm that rises to the level of significance required for notification….The extracted information is insufficient for identity theft….There is similarly, minimal, if any risk of other financial harm based on the nature of the extracted information….While Uber is monitoring the accounts whose data was included in the downloaded files and has flagged them for additional fraud protection, it has not seen evidence of fraud or misuse tied to the incident." Regarding the potential harm of phishing, the Organization reported "there is no causal relationship such that the release of email addresses in these circumstances could be said to be a real risk of significant harm as a result of the incident. Phishing, phone scams and other fraudulent practices are a recognized consequence of living in the digital age, not as a result of a data incident….Any potential harm from phishing results as a consequence of the individual him or herself supplying personal information such as access codes and passwords, and not the consequence of having received such an email." In my view, a reasonable person would consider that the identity information of drivers (specifically driver's license numbers), particularly in combination with other personal information elements at issue, could be used to cause the harms of identity theft and fraud. These are significant harms. Further, particularly when combined with profile information (e.g. information that individuals are customers/drivers), individual names, mobile telephone numbers and email addresses of riders and drivers could be used to send sophisticated, user-specific emails

	and text messages purportedly from the Organization (phishing, smishing or SMS/text phishing). Merely clicking on a link, without a user providing any additional information, could potentially cause significant harm (e.g. activate malware, infect users' computer/networks). In breach notification decision #P2011-ND-011, the former Commissioner said that "…a small…portion of affected individuals are likely to either open attachments with malware or be tricked into providing additional information. This is the known pattern that is used by criminals when attempting to obtain personal information. Phishing attacks have been successful in the past and there is no evidence to indicate that the information obtained through the…breach will be treated any differently." Despite individuals being increasingly aware of the possibility of receiving phishing emails and texts, incidents of phishing occur with regularity as evidenced by the breaches reported to my office. Further, as smartphones are one of the primary means to access the Organization's services, the Organization's users may be particularly vulnerable to these types of harms. Consistent with the reasoning in breach notification decision #P2011-ND-011, and many decisions posted on my office's website since, I find a reasonable person would consider phishing/smishing to be a significant harm.
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 said that "the breach does not pose a real risk of significant harm…the information at issue was not sensitive in nature and any exposure was quickly contained…". In addition, the Organization stated that "the recipients of the information as well as the location of the information once extracted were quickly identified by Uber….Uber identified the real names and identities of the outside actors and met in person with both individuals. Uber believed that making it known that they knew the true identity of such individuals was a strong deterrent to their engaging in any undesired actions. Uber's security team paid the outside actors to destroy the data, as demanded…and obtained assurances from the individuals that they had destroyed and would not use or further disseminate the downloaded information, and to the best of Uber's knowledge, such materials were destroyed. This included engaging in communications with them regarding how they had deleted the data to confirm that the explanation made sense from a technical perspective." In my view, the likelihood of significant harm resulting from this incident is increased because the personal information was

	compromised due to a deliberate unauthorized intrusion by third party individuals. Although the Organization said that the incident was "quickly contained" and additional safeguards were implemented, it is nonetheless the case that the unauthorized third parties controlled the personal information of millions of users for approximately a month or longer. The additional safeguards were implemented after the personal information was already compromised. Uber did not contract a cyber security forensic company to analyze the data that was downloaded until almost a year after the original incident. Despite receiving assurances from the unauthorized third parties that the personal information would not be used or further disseminated, the fact remains that these assurances were given by individuals who deliberately accessed the information without authority, made ransom demands, and accepted payment of a ransom. These factors weigh heavily against accepting or trusting assurances from the third parties. Further, although the Organization said the unauthorized third parties assured Uber that the information had been deleted and would not be used or <u>further</u> disseminated, it not clear whether the information had already been disseminated. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, identity theft and fraud can occur months and even years after a data breach.

DECISION UNDER SECTION 37.1(1) OF PIPA

In my view, based on the information provided by the Organization and given the circumstances of the incident, a reasonable person would consider that there is a real risk of significant harm to the affected individuals as a result of the incident.

The identity information of drivers (specifically driver's license numbers), particularly in combination with other personal information elements at issue, could be used to cause the harms of identity theft and fraud. These are significant harms.

Further, particularly when combined with profile information (e.g. information that individuals are customers/drivers), individual names, mobile telephone numbers and email addresses of riders <u>and</u> drivers could be used to send sophisticated, user-specific emails and text messages purportedly from the Organization (phishing, smishing or SMS/text phishing). Merely clicking on a link, without a user providing any additional information, could potentially cause significant harm (e.g. activate malware, infect users' computer/networks).

In breach notification decision #P2011-ND-011, the former Commissioner said that "…a small…portion of affected individuals are likely to either open attachments with malware or be tricked into providing additional information. This is the known pattern that is used by criminals when attempting to obtain

personal information. Phishing attacks have been successful in the past and there is no evidence to indicate that the information obtained through the…breach will be treated any differently."

Despite individuals being increasingly aware of the possibility of receiving phishing emails and texts, incidents of phishing occur with regularity as evidenced by the breaches reported to my office. Further, as smartphones are one of the primary means to access the Organization's services, the Organization's users may be particularly vulnerable to these types of harms.

Consistent with the reasoning in breach notification decision #P2011-ND-011, and many decisions posted on my office's website since, I find a reasonable person would consider phishing/smishing to be a significant harm.

The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate unauthorized intrusion by third party individuals.

Although the Organization said that the incident was "quickly contained" and additional safeguards were implemented, it is nonetheless the case that the unauthorized third parties controlled the personal information of millions of users for approximately a month or longer. The additional safeguards were implemented after the personal information was already compromised. Uber did not contract a cyber security forensic company to analyze the data that was downloaded until almost a year after the original incident.

Despite receiving assurances from the unauthorized third parties that the personal information would not be used or further disseminated, the fact remains that these assurances were given by individuals who deliberately accessed the information without authority, made ransom demands, and accepted payment of a ransom. These factors weigh heavily against accepting or trusting assurances from the third parties.

Further, although the Organization said the unauthorized third parties assured Uber that the information had been deleted and would not be used or further disseminated, it not clear whether the information had already been disseminated.

The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, identity theft and fraud can occur months and even years after a data breach.

I require the Organization to notify affected individuals whose personal information was collected in Alberta (drivers and riders) in accordance with section 19.1 of the Personal Information Protection Act Regulation (Regulation) and notify me in writing that it has done so within 10 days of the date of this decision. The Organization is not required to notify drivers whom it has already notified in compliance with the Regulation.

Jill Clayton
Information and Privacy Commissioner