Published under Section 48(2) of the
Personal Data (Privacy) Ordinance (Cap. 486)

Investigation Report:

HKA Holidays Limited Leaked Customers' Personal Data through the Mobile Application "TravelBud"

Report Number: R14 – 6453

Date issued: 15 December 2014

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

HKA Holidays Limited leaked customers’ personal data through the Mobile Application “TravelBud”

This report in respect of the investigation carried out by the Privacy Commissioner for Personal Data (the “**Commissioner**”) pursuant to section 38(b) of the Personal Data (Privacy) Ordinance, Cap. 486 (the “**Ordinance**”) against HKA Holidays Limited is published in the exercise of the power conferred on the Commissioner by Part VII of the Ordinance. Section 48(2) of the Ordinance provides that *“the Commissioner may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report –*

(a) setting out -

(i) the result of the investigation;

(ii) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(iii) such other comments arising from the investigation as he thinks fit to make; and

(b) in such manner as he thinks fit.”

ALLAN CHIANG
Privacy Commissioner for Personal Data

Investigation Report: HKA Holidays Limited leaked customers' personal data through the Mobile Application "TravelBud"

This is a report of an investigation prompted by a data breach incident concerning the leakage of personal data of the customers of HKA Holidays Limited ("HKA Holidays") through its mobile application "TravelBud" running on iOS platform. The Privacy Commissioner for Personal Data found that HKA Holidays had contravened Data Protection Principle 4 under the Personal Data (Privacy) Ordinance for having failed to take all reasonably practicable steps to ensure that customers' personal data was protected against unauthorised or accidental access.

Background

HKA Holidays Limited ("**HKA Holidays**"), the then subsidiary company of Hong Kong Airlines Limited, developed and operated a mobile application ("**app**") TravelBud[1] ("**TravelBud**") since 2010. TravelBud is a travel assistant app providing online services to mobile device users including flight ticket reservation and purchase, flight itinerary management, search for information on destination, and provision of a social networking platform for the travellers.

2. On 30 September 2013, HKA Holidays submitted a "Data Breach Notification Form" to this Office reporting that the personal data of six of its customers was leaked on 19 September 2013 through TravelBud running on iOS platform[2]. The personal data leaked in the incident included customers' name, identity card or passport number, gender, telephone number, email address and date of birth.

3. The breach was discovered on 25 September 2013 when Hong Kong Airlines Limited received a complaint in relation to the data leakage in TravelBud from a customer. The company notified HKA Holidays on the same day.

4. The Privacy Commissioner for Personal Data (the "**Commissioner**")

[1] According to the App Store of Apple Inc., the name of this mobile application was「俠客行·旅行 (TravelBud)」.

[2] A mobile operating system developed by Apple Inc. and distributed exclusively for Apple Inc.'s mobile device.

followed up by initiating an investigation against HKA Holidays pursuant to section 38(b) of the Personal Data (Privacy) Ordinance (the "**Ordinance**").

<u>Relevant Provisions of the Ordinance</u>

5. The Ordinance seeks to protect the privacy of individuals in relation to personal data. It imposes obligations on data users to comply with the six data protection principles in Schedule 1. The term "data user" is defined under section 2 of the Ordinance to mean a person who, either alone or jointly or in common with others, controls the collection, holding, processing or use of the personal data. Of relevance to this investigation is Data Protection Principle ("**DPP**") 4 in Schedule 1 to the Ordinance and section 65 of the Ordinance. DPP4 provides:-

> " *(1) All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to –*
>
> *(a) the kind of data and the harm that could result if any of those things should occur;*
> *(b) the physical location where the data is stored;*
> *(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;*
> *(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and*
> *(e) any measures taken for ensuring the secure transmission of the data.*
>
> *(2) Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.*"

6. According to section 2 of the Ordinance, "practicable" means

reasonably practicable.

7. Section 65(2) of the Ordinance stipulates that:-

> "*Any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of this Ordinance as done or engaged by that other person as well as by him.*"

Information collected during the Investigation

8. In the course of this investigation, this Office made enquiries with HKA Holidays and examined the documentary evidence provided by them. Below is the relevant information obtained by this Office.

Development and Operation of TravelBud

9. TravelBud runs on two platforms: Android developed by Google Inc. and iOS developed by Apple Inc.. It was first launched on these two platforms on 24 July 2012 and 4 September 2012 respectively. The incident concerns TravelBud running on iOS platform only.

10. HKA Holidays had outsourced the development of TravelBud to BBDTEK Company 佰邦達科技(北京)有限公司 ("**BBDTek**"), a Mainland-based software development vendor which also provided maintenance support, bug fixing and version upgrade for TravelBud software upon HKA Holiday's request. No personal data of customers of HKA Holidays was provided or entrusted to BBDTek for processing or testing during the development or subsequent maintenance of TravelBud. In addition, BBDTek had no access to the backend database of TravelBud which contained the personal data of HKA Holidays' customers.

Use of TravelBud and the user identifiers

11. TravelBud supported two types of users with browsing and access rights: members and non-members. At the time of the incident, there were approximately 25,000 members using TravelBud. Approximately 40,000 transactions and 80,000 enquiries were made through TravelBud by members and

non-members combined during the period between July 2012 and June 2014.

12. Non-members could browse and access most of the functions provided by the app, including flight ticket and annual pass[3] reservation and purchase, and order history enquiry. During the reservation process, non-members were required to provide passengers' personal data, including their full name, gender, date of birth, and identity card or passport number, and contact persons' personal data, including their name, telephone number and email address.

13. Personal data provided for first-time reservation and purchase of flight tickets and annual pass were stored in TravelBud's backend database. For future access to the system for reserving or purchasing tickets and making order enquiries, they could skip the process of personal data re-entry. This was made possible by HKA Holidays' use of the unique MAC address[4] of a mobile device as the parameter for associating TravelBud's backend database with the non-member's particular mobile device used for inputting passengers' personal data at the outset.

14. Members, on the other hand, could browse and access all the functions of TravelBud and enjoy discounts on purchasing flight tickets or annual pass through this channel. To register as members, users were required to create user login accounts by providing their email addresses and passwords. Alternatively, they could create user login accounts based on their existing social network accounts[5]. TravelBud could identify each individual member by the user login account data.

15. Members were required to input the same types of personal data mentioned in paragraph 12 above when they reserved or purchased flight tickets and annual pass for the first time. For subsequent transactions, including order enquiries, the user login procedure obviates the need for re-entry of the personal data.

16. The following table summarises the core functions of TravelBud available to members and non-members, and the means of identifying the

[3] A package of several flight tickets which could be used over a one-year period.

[4] A media access control address ("**MAC address**") is a unique identifier assigned to network interfaces for communications on the physical network segment. It is a 48-bit hexadecimal number most often assigned by the manufacturer of a network interface and exists on all mobile computing devices with network connectivity.

[5] TravelBud accepts Tencent and Sina accounts for registration.

respective users :-

	Functions of TravelBud	**Members**	**Non-members**
(1)	Reservation and purchase of flight tickets	✓	✓
(2)	Purchase of annual pass	✓	✓
(3)	Redemption of annual pass	✓	✗
(4)	Order history enquiry	✓	✓
The identification parameter used to associate the backend database with the user		User login data	MAC address

Security measures of TravelBud

17. All personal data collected by TravelBud was stored in its backend database server, physically hosted in an outsourced data centre in Beijing, China. HKA Holidays confirmed that, except for the member login passwords, the personal data contained in its backend database server was not encrypted.

Cause of the data breach

18. When a non-member user first reserved or purchased a flight ticket or annual pass, TravelBud would ask the iOS operating system of the non-member's mobile device, regardless of its version, to provide the device's MAC address. This MAC address would then be recorded in the backend database of TravelBud.

19. When the same user made further attempts to reserve or purchase a flight ticket or annual pass, or performed an order history enquiry, TravelBud would obtain the MAC address of his[6] mobile device again and check it against the backend database for identifying the user. After successful matching, the previously stored information corresponding to the MAC address would be retrieved from the database and displayed on the mobile device. The following subparagraphs describe the information that were displayed after successful matching:-

19.1 <u>Reservation of flight tickets</u>

[6] Words and expressions importing the masculine gender include the feminine gender in this report.

After inputting the personal data and completing the reservation, the full name and identity card or passport number of the passenger would be displayed under the heading “historical passenger” while the name and telephone number of the contact person would be displayed under the heading “historical contact person” on the same screen. For further reservation and purchase transactions, users could access and update the information by clicking into the “historical passenger” or “historical contact person” links.

19.2 Purchase of annual pass

Similar to the reservation of flight tickets, after inputting the personal data and completing the purchase of annual pass, “historical passenger” and “historical contact person” information would be created and thereafter could be accessed and updated.

19.3 Order history enquiry

Through the “order history enquiry” function, the user could review the status of his orders, including the order date, payment process, flight tickets issuance and cancelled orders.

20. This mechanism worked fine for mobile devices running on iOS6 and earlier versions. Please refer to **Annex A** for more details on the matching between the mobile devices and backend database for iOS6 and earlier versions.

21. On 18 September 2013 (US time), Apple Inc. launched its new mobile operating system iOS7 and users were able to upgrade their mobile devices to iOS7 with effect from the same date. For reason of privacy protection, iOS7 blocked the reading by apps of MAC address as a mobile device identification parameter. In response to apps asking for the MAC address of a mobile device, iOS7 would provide a fixed number instead of disclosing the true MAC address.

22. Consequently, whenever a non-member reserves or purchases a flight ticket or annual pass through TravelBud on a mobile device running on iOS7, iOS7 would return the same fictitious MAC address[7]. This number address

[7] The fixed MAC address in iOS7 is: 02:00:00:00:00:00.

holds constant for all mobile devices running on iOS7. In the circumstances, all non-members making transactions under iOS7 environment were identified as one person based on the same fictitious MAC address.

23. As a result, during the period from 19 to 25 September 2013 (Hong Kong time), in response to a non-member attempting to reserve or purchase a flight ticket or annual pass, or made an order history enquiry using a mobile device operating on iOS7, TravelBud would return not only his records (order histories and personal data) but also those of other non-members who had made transactions through TravelBud under iOS7. In the incident, there was a total of six affected customers whose personal data was leaked to other non-members in this way. Non-members using iOS6 or earlier iOS versions were not affected. Please refer to **Annex B** for a demonstration of the operation of TravelBud running on iOS7, in particular the failure to match the mobile devices running on iOS7 with TravelBud's backend database.

The Findings of the Commissioner

24. In accordance with DPP4, data users are obliged to take all reasonably practicable steps to ensure that personal data is protected against unauthorised or accidental access, having particular regard to the kind of data and the harm that could result if such event should occur. While DPP4 does not require a data user to provide an absolute guarantee for the security of the personal data held by it, the Commissioner had to consider whether HKA Holidays had taken all reasonably practicable measures to protect the personal data when operating TravelBud.

Whether HKA Holidays and BBDTek had promptly responded to the change in the operating environment of mobile devices

25. HKA Holidays had outsourced the development of TravelBud to BBDTek as stated in paragraph 10 above. During our investigation, HKA Holidays claimed that prior to the incident, HKA Holidays was responsible for initiating changes to TravelBud's functions and features, while BBDTek was responsible for updating the app and checking relevant latest information from Apple Inc. on a weekly basis. BBDTek admitted that it had not taken any action

Reference:
https://developer.apple.com/library/IOs/releasenotes/General/RN-iOSSDK-7.0/index.html#//apple_ref/doc/uid/TP40013202-CH1-SW33

to update TravelBud until the leakage was discovered on 25 September 2013.

26. The Commissioner notes that the change to the MAC address behaviour on iOS7 helped to protect users' privacy by preventing users from being persistently tracked by apps without their knowledge or consent. Apple Inc. first notified the app developers of the impending release of iOS7 at its Worldwide Developer Conference ("**WWDC**") held in San Francisco, the United States on 10 June 2013. All the presentation materials from WWDC explaining the new MAC address behaviour were made available online shortly after the event. Apple Inc. subsequently communicated this change to its paid app developers[8] ("**Paid Developers**") and other registered app developers through email.

27. On 22 August 2013, Apple Inc. reiterated the change and impact of the MAC address behaviour through a public announcement in the dedicated developer platform to all registered app developers (whether paid or not):-

> "*If your apps use the MAC address to identify an iOS device, the system will return the same static value for all devices running iOS7. Please update your apps to use the identifierForVendor property of UIDevice. If you need an identifier for advertising purposes, use the advertisingIdentifier property of ASIdentifierManager.*"

28. Moreover, a total of six iOS7 beta versions were made available to Paid Developers for testing their apps from the date of the WWDC on 10 June 2013 to the date of the official launch of iOS7 on 18 September 2013.

29. However, BBDTek submitted via HKA Holidays that it had only registered with the iOS Developer Program in September 2013 and had not received any notification from Apple Inc. in relation to the release of iOS7. It claimed that it first obtained such information through Apple Inc.'s public announcement on 11 September 2013 that iOS7 would be officially released on 18 September 2013.

30. The Commissioner finds it difficult to accept BBDTek's claim of

[8] They are app developers registered with Apple Inc.'s iOS Developer Program and paid yearly subscription fee. Paid Developers enjoy advanced developer tools and support from Apple Inc. and would receive email updates and notifications from Apple Inc. App developers may also register as an Apple developer for free, thus gaining access to certain developer tools and resources for creating iOS apps and Apple Inc.'s public announcements.

ignorance. It is inconceivable that BBDTek, as a technology company specialising in app development, was unaware of Apple Inc.'s notification or news in relation to the changes or updates of the mobile operating system until 11 September 2013. Even though BBDTek only registered with the iOS Developer Program in September 2013 and would not have received relevant email notification from Apple Inc., it should have kept abreast of the news and technology updates from Apple Inc.

31. In fact, Apple Inc.'s three months' advance notice of launching new iOS version (from WWDC on 10 June 2013 to the official release on 18 September 2013) was usual practice in line with previous iOS releases. The Commissioner considers that Apple Inc. had given ample notice to all app developers of when iOS7 would be introduced and what the changes in relation to MAC address were. By repeated communication through various channels and providing app developers with access to the pre-released beta version of iOS7, Apple Inc. has done its fair share of work to ensure that none of the existing apps would be adversely affected by the changes.

32. Further, even if it was true that BBDTek became aware for the first time of the release of iOS7 on 11 September 2013, there was still time for BBDTek to take steps to prevent the data breach as iOS7 was launched a week later on 18 September 2013.

33. In view of the above, the Commissioner concludes that BBDTek failed to respond to the change of MAC address behaviour, thus causing the leakage incident. For an app development company that has been paid to maintain an app it has developed, BBDTek obviously has failed its duty. However, BBDTek was only an outsourced agent in this incident. HKA Holidays had not provided or entrusted any personal data of its customers to BBDTek for processing or testing during the development or subsequent maintenance of TravelBud software nor was it allowed to have access to the backend database of TravelBud. Accordingly, BBDTek was not a data user as defined under the Ordinance as it has no control in the collection, holding, processing or use of the personal data. Therefore, the Commissioner cannot take direct enforcement action against it.

34. However, by virtue of section 65(2) of the Ordinance, any act done or practice engaged in by an agent for another person with the latter's authority shall be treated as done or engaged in by both the agent and that other person. For this reason, even though HKA Holidays had outsourced the task of

development and maintenance of TravelBud to BBDTek, HKA Holidays as the data user remains accountable for the unauthorised or accidental access of personal data that had taken place.

Conclusion

35. Based on the above findings and analysis, the Commissioner determines that HKA Holidays had contravened DPP4(1) for having failed to take all reasonably practicable steps to ensure that the personal data it handled through the operation of TravelBud was protected against unauthorised or accidental access.

Remedial Action

36. Pursuant to section 50(1) of the Ordinance and in consequence of an investigation, if the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, he may serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent any recurrence of the contravention.

37. On 25 September 2013, upon receiving a customer's complaint, HKA Holidays immediately suspended the annual pass purchase function and the order enquiry function for non-members of TravelBud. Therefore, non-members could not access any "historical passenger" and "historical contact person" information through TravelBud. Subsequently, HKA Holidays duly notified all the affected individuals in the incident and no further complaint was received.

38. On 1 October 2013, HKA Holidays released an updated version of TravelBud for running on iOS platform, which had the following remedial features:-

(i) MAC address was no longer used as the identification parameter of mobile devices for non-members who reserved and purchased flight tickets through TravelBud;

(ii) The enquiry function of "historical passenger" and "historical contact person" information for non-members through TravelBud was disabled;

(iii) The order history enquiry function for non-members was disabled. Only members could make order history enquiry through user login account;

(iv) Purchase and redemption of annual pass tickets was only available to members who used their user login account for login; and

(v) Non-members could still purchase flight tickets but needed to provide personal data of passenger(s) and contact person(s) for each purchase.

39. On 12 October 2013, HKA Holidays also applied the measures in paragraph 38 to the version of TravelBud running on Android platform.

40. Given that HKA Holidays had abolished the use of MAC address as the identification parameter, disabled the enquiry functions of "historical passenger" and "historical contact person" information and the order history enquiry function for non-members, and restricted the purchase of annual pass tickets to members only, the Commissioner considers that HKA Holidays has taken adequate steps to remedy the contravention and to prevent its recurrence.

41. The Commissioner further notes that the legal ownership of TravelBud had been transferred from HKA Holidays to a Mainland company called Grand China Express International Travel Service Co Ltd[9] in January 2014, and as a result the ongoing development and maintenance of TravelBud would henceforth take place outside the jurisdiction of Hong Kong.

42. In the circumstances, no enforcement notice has been served on HKA Holidays. However, the Commissioner has put HKA Holidays on WARNING that if it fails to observe the relevant requirements of the Ordinance in similar situations in future, he may consider taking enforcement action against HKA Holidays including the serving of an enforcement notice.

Other Comments

Advice to app developers and organisations which outsource app development

43. Apps are now commonplace tools, transforming business operations and individuals' lives. People use apps on their mobile devices constantly, such as to check their account balance, to shop, to watch news and to communicate

[9] Both HKA Holidays and Grand China Express International Travel Service Co Ltd are subsidiaries of a company incorporated in Mainland China.

instantly with their friends and relatives, etc. App developers often collect and process a wide range of personal data through the apps. Hence they play a key role in safeguarding privacy in the use of mobile devices. Although they are mostly small and medium enterprises, they still have the obligation to comply with the requirements under the Ordinance. They are advised to take advantage of the seminars and best practice guide provided by the Commissioner. It is also incumbent upon them to keep abreast of the relevant trends and developments in technology so that they can update the apps they have developed to achieve enhanced functionality without compromising privacy and data protection.

44. When outsourcing the development of the apps, organisations should exercise care and choose competent app developers with good track records. Without appropriate safeguards in appointing outsourced agents, leakage or misuse of the personal data contained therein due to the agents' negligence might happen, thus causing serious harm to its customers and bringing the company into disrepute.

Measures to be adopted when engaging an outsourced app developer

45. DPP4(2) of the Ordinance requires that if a data user engages a data processor to process personal data on its behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing. According to DPP2(4) of the Ordinance, "data processor" means a person who processes personal data on behalf of another person and does not process the data for any of the person's own purposes.

46. In the present case, BBDTek was not a data processor as defined under DPP2(4) as HKA Holidays engaged BBDTek to develop and maintain TravelBud software without providing or entrusting any personal data to it. However, the negligence of BBDTek in failing to update the app had compromised the customers' data of HKA Holidays.

47. While DPP4(2) has no direct application to the present incident, a data user is obligated under DPP4(1) to take all reasonably practicable steps to safeguard the security of personal data. The Commissioner advises that a data user in engaging an outsourced app developer has to adopt contractual or other

means to require the app developer[10]:-

(i) To have in place proper application development and change-control policy, guidelines and procedures;
(ii) To have in place risk assessment process for the design and operation of applications;
(iii) To use genuine and reliable development tools and software;
(iv) To maintain safeguards, such as encryption, access control, password policy;
(v) To establish processes to access or obtain updates from the operating system developers;
(vi) Where justified, to be subject to review and audit by the data users or an independent party; and
(vii) Not to subcontract or further outsource the work unless the same level of protection could be assured.

Encryption of personal data

48. The Commissioner noted that all personal data contained in the backend database server of TravelBud was not encrypted, except for the password of user login account. Although this was not the direct cause of the leakage incident, a prudent data user is advised to ensure that sensitive personal data (e.g. identity card and passport number) stored in the backend servers is protected by access control and encryption. These measures could avoid unauthorised data access and minimise harm caused to data subjects in the event of a data leakage.

[10] See for reference the requirements for outsourcing the processing of personal data to agents in the Information Leaflet "*Outsourcing the Processing of Personal Data to Data Processors*" issued by this Office in September 2012.