

NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
799 9th Street NW
Suite 1000
Washington, DC 20001-4501
United States

Chris Cwalina
Partner

Direct line 202 662 4691
chris.cwalina@nortonrosefulbright.com

Tel +1 202 662 0200
Fax +1 202 662 4643
nortonrosefulbright.com

October 25, 2018

Via Email (attorneygeneral@doj.nh.gov)

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

Pursuant to N.H. Rev. Stat. §359-C:20, we write on behalf of our client, Cathay Pacific Airways Limited (“**Cathay**”), to notify you of a security incident that affected the personal information of certain New Hampshire residents.¹ At this time, Cathay has no evidence that any New Hampshire residents’ personal information has been misused.

Timeline

On March 13, 2018, Cathay first detected suspicious activity on its network and took immediate action to contain the event, and commence an internal investigation with the assistance of Mandiant, a leading cybersecurity firm, to investigate the event thoroughly.

On May 7, 2018, Cathay’s forensic investigators confirmed that there had been unauthorized access to some of its information systems containing passenger data. Upon confirming

¹ Personal data of passengers of Cathay Pacific and Hong Kong Dragon Airlines Limited were affected. Hong Kong Dragon Airlines Limited is a wholly owned subsidiary of Cathay Pacific and the personal data of Hong Kong Dragon Airlines Limited passengers resides on Cathay Pacific’s information systems. In an addition, members of Asia Miles were affected by this event. Asia Miles also is owned by, and provided to members by Cathay Pacific, and is managed and operated by Asia Miles Limited, a wholly owned subsidiary of Cathay Pacific, as an agent of Cathay Pacific. This notice is made by Cathay Pacific on behalf of the aforementioned group entities.

unauthorized access, the investigation focused on determining: (1) which personal data had been accessed; (2) whether data had been accessed/ viewed within Cathay's information systems; (3) whether there was any evidence that the data had been exfiltrated from Cathay's information systems; and (4) whether the data in question could be reconstructed outside of Cathay's information systems allowing the personal data to be useable and readable to the unauthorized third party.

Upon making the finding that the data in question had been accessed and /or exfiltrated and was potentially readable to the unauthorized and unknown third party, Cathay continued its analysis to identify the individuals who may have been affected, so that appropriate information could be provided to those individuals.

Cathay has very recently established the types of personal data involved and confirmed that personal information, as defined under N.H Rev. Stat. §359-C:19, had been accessed.

Cathay is notifying the individuals it was able to identify, however, due to Cathay's inability to identify all potentially affected New Hampshire residents, Cathay is also providing substitute notice. Cathay has also notified the Hong Kong Police.

Data Involved

Personal data of passengers of Cathay and Hong Kong Dragon Airlines Limited ("**Cathay Dragon**") were affected. Cathay Dragon is a wholly owned subsidiary of Cathay and the personal data of Cathay Dragon passengers resides on Cathay's information systems.

Members of Asia Miles were affected by this event. Asia Miles is owned by, and provided to members by Cathay, and is managed and operated by Asia Miles Limited, a wholly owned subsidiary of Cathay, as an agent of Cathay.

The following types of personal data of New Hampshire residents was accessed: nationality; date of birth; phone number; email; address; passport number; frequent flyer membership number; customer service remarks; and historical travel information. Please note that the combination and number of personal data elements accessed varies for each affected passenger.

Number of Affected New Hampshire Residents and Method of Notice

Cathay has identified the contact information of seven (7) New Hampshire individuals and these individuals will be notified via U.S. mail in the next few days. A form copy of this letter is included for your reference. For other individuals who Cathay is unable to contact and who believe they may have been affected, Cathay has set up a dedicated website at infosecurity.cathaypacific.com to provide information about the event and measures that affected individuals can take to protect themselves. Individuals may check if they have been affected by registering an enquiry with Cathay via the website. This website went live on October 25, 2018. A form copy of the substitute notice provided on this website is also attached for your reference. Cathay has also issued a press release to the media on this matter.

Assistance Offered

Because Cathay takes the privacy of personal information very seriously, and regrets that this type of information was vulnerable, Cathay is notifying the affected New Hampshire residents and has engaged Experian to provide identity monitoring services to affected individuals. This service (IdentityWorks Global Internet Surveillance) monitors if an individual's personal data may be available on public websites, chat rooms, blogs, and non-public places on the internet where data can be compromised such as dark web sites.

In addition, Cathay has set up the following channels for affected individuals to contact it:

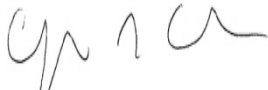
- a dedicated customer care center for one (1) month for which a toll free number has been set up; and
- a dedicated email at infosecurity@cathaypacific.com.

Remediation

To help prevent a similar incident from occurring in the future, Cathay has enhanced the security and monitoring of its environment and is working with the forensic investigation firm referenced above, as well as other cybersecurity experts, to implement measures to prevent future unauthorized access to its systems and databases, as well as further enhance its IT security generally.

If you have any questions or need further information regarding this incident, please contact me at (202) 662 4691 or chris.cwalina@nortonrosefulbright.com.

Very truly yours,



Chris Cwalina

CGC/

Enclosure

Official emails relating to this data security event will be sent from an address with the format infosecurity@cathaypacific.com.

With regard to this data security event, we will never request your personal or financial information, and we will never ask for your password.

If you are concerned about an email, we recommend that you don't click on any links, open any attachments or reply to it.

[Date]

[Insert Recipient's Name]

[Insert Address]

[Insert City, State, Zip]

RE: Notice of Data Breach

Dear [Insert Recipient's Name]:

We are contacting you to make you aware of a data security event that involves some of your personal information. We are very sorry for any concern that this event may cause you, and this notice will provide you with information about what happened and how we can assist you.

What Happened.

We initially discovered suspicious activity on our network in March this year. Upon discovery, we took immediate action to contain the event, to commence a thorough investigation with the assistance of a leading cybersecurity firm, and to further strengthen our IT security measures. Unauthorised access to certain personal data was confirmed in early May. Since that time, analysis of the data has continued in order to identify affected individuals and to determine whether the data at issue could be reconstructed.

We have no evidence that any personal information has been misused. We recommend that you follow the steps outlined in this notice to help protect yourself against potential risks.

What Information Was Involved.

The following personal information about you was accessed: [insert].

Your travel or loyalty profile was not accessed in full, and your password was not compromised.

What We Are Doing.

You can find more information at our dedicated website, infosecurity.cathaypacific.com.

We are offering ID monitoring services to affected passengers and this will be provided by Experian, a global data and information service provider. This service (IdentityWorks Global Internet Surveillance) monitors if your personal data may be available on public websites, chat rooms, blogs, and non-public places on the internet where data can be compromised such as dark web sites.

This is an optional service, and how much information to include in the identity monitoring is completely at your discretion.

The information you provide to Experian will only be used by Experian for the sole purposes of identity monitoring. It will not be published to any other entity.

Please visit the following website: <http://www.globalidworks.com/identity1> and click the Get Started button to activate this 12 month complimentary service. You can then enter your personalized activation code: [Inserted Activation code] to start your IdentityWorks Global Internet Surveillance.

We have notified, or are notifying, the relevant authorities and the Hong Kong Police.

What You Can Do.

Although no-one's travel or loyalty profile was accessed in full and no passwords were compromised, as best practice, we recommend that you consider:

- changing your passwords regularly;
- checking for any suspicious activity; and
- being vigilant against phishing or other attempted scams.

As mentioned above, we are offering ID monitoring services to affected passengers. Please visit the following website: <http://www.globalidworks.com/identity1> and click the Get Started button to activate this 12 month complimentary service using your personalized activation code above

For information on passport replacements please see the State Department's website regarding lost or stolen passports at <https://travel.state.gov/content/travel/en/passports/after/lost-stolen.html>.

We also recommend that our passengers remain vigilant with respect to reviewing account statements and monitoring credit reports for unauthorized activity, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). In addition, we have provided supplemental information regarding further actions you may consider and resources to obtain additional information about identity theft and ways to protect yourself.

For More Information.

If you have any further questions about the event, you can contact us by:

- visiting our dedicated website at infosecurity.cathaypacific.com;
- calling our dedicated call center at 1-888-229-5139; or
- emailing us at infosecurity@cathaypacific.com.

We want to reassure you that there is no impact on flight safety as the IT systems affected were totally separate from our flight operations systems, and that we took and continue to take measures to enhance our IT security. Your safety and security remains our top priority.

Yours sincerely,

Rupert Hogg
Chief Executive Officer
Cathay Pacific Airways Limited

For your information:

Asia Miles is owned by, and provided to members by Cathay Pacific Airways Limited, and is managed and operated by Asia Miles Limited, a wholly owned subsidiary of Cathay Pacific Airways Limited, as an agent of Cathay Pacific Airways Limited.

Hong Kong Dragon Airlines Limited is a wholly owned subsidiary of Cathay Pacific Airways Limited and Cathay Pacific Airways Limited manages and provides IT support services to Hong Kong Dragon Airlines Limited.

The Activation Code for the ID Monitoring Services will expire on 30 April 2019.

Additional Information

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Security Freeze. You have the ability to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent

utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is \$5.

For Rhode Island residents: The credit bureaus may require you to pay a fee to place, lift, or remove the security freeze.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.

Number of Rhode Island Residents Affected: Approximately 1.

October 25, 2018

IMPORTANT INFORMATION: DATA SECURITY EVENT

Official emails relating to this data security event will be sent from an address with the format infosecurity@cathaypacific.com.

With regard to this data security event, we will never request your personal or financial information, and we will never ask for your password.

If you are concerned about an email, we recommend that you don't click on any links, open any attachments or reply to it.

We would like to inform you of a data security event that may involve some of your personal data. We are very sorry for any concern that this event may cause you, and this notice will provide you with information about what happened and how we can assist you.

What Happened.

We initially discovered suspicious activity on our network in March this year. Upon discovery, we took immediate action to contain the event, to commence a thorough investigation with the assistance of a leading cybersecurity firm, and to further strengthen our IT security measures. Unauthorised access to certain personal data was confirmed in early May. Since that time, analysis of the data has continued in order to identify affected individuals and to determine whether the data at issue could be reconstructed.

We have no evidence that any personal data has been misused. We recommend that you follow the steps outlined in this notice to help protect yourself against potential risks.

What Information Was Involved.

The following types of personal data of Cathay Pacific and Cathay Dragon passengers was accessed: name; nationality; date of birth; phone number; email; address; passport number; frequent flyer programme membership number; customer service remarks and historical travel information.

The combination of data accessed varies for each affected passenger.

No-one's travel or loyalty profile was accessed in full, and no passwords were compromised.

What Are We Doing.

We are contacting affected passengers to provide information on steps that you can take to protect yourself. If you are an affected member of the Marco Polo Club, Asia Miles or a Registered User, you will be contacted individually in the coming days. In that communication, we will tell you which specific types of personal information about you may have been accessed.

If you believe you may have been affected, you can submit a request [here](#) and we will tell you if we have identified your personal data as having been accessed.

We are offering ID monitoring services to affected passengers and this will be provided by Experian, a global data and information service provider. This service (IdentityWorks Global Internet Surveillance) monitors if your personal data may be available on public websites, chat rooms, blogs, and non-public places on the internet where data can be compromised such as dark web sites. If you are an affected member of the Marco Polo Club, Asia Miles or a Registered User, we will contact you individually with relevant information.

We have notified, or are notifying, the relevant authorities and the Hong Kong Police.

What You Can Do.

Although no-one's travel or loyalty profile was accessed in full and no passwords were compromised, as best practice, we recommend that you consider:

- changing your passwords regularly;
- checking for any suspicious activity; and
- being vigilant against phishing or other attempted scams.

As mentioned above, we are offering ID monitoring services to affected passengers. If you are an affected member of the Marco Polo Club, Asia Miles or a Registered User, we will contact you individually with relevant information. If you are not sure if you are affected, please register your enquiry with us on infosecurity.cathaypacific.com and we will get back to you.

For information on passport replacements please see the State Department's website regarding lost or stolen passports [here](#).

We also recommend that our passengers remain vigilant with respect to reviewing account statements and monitoring credit reports for unauthorized activity, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). In addition, we have provided supplemental information regarding further actions you may consider and resources to obtain additional information about identity theft and ways to protect yourself.

For More Information.

If you have any further questions about the event, more information is available at [Link to FAQ page of website], or you can:

- call our customer care center at 1-888-229-5139. The number will be available from 12:30 pm Hong Kong time on 25 October 2018; or
- email us at infosecurity@cathaypacific.com.

We want to reassure you that there is no impact on flight safety as the IT systems affected are totally separate from our flight operations systems, and that we took and continue to take measures to enhance our IT security. Your safety and security remains our top priority.

For your information:

Asia Miles is owned by, and provided to members by Cathay Pacific Airways Limited, and is managed and operated by Asia Miles Limited, a wholly owned subsidiary of Cathay Pacific Airways Limited, as an agent of Cathay Pacific Airways Limited.

Hong Kong Dragon Airlines Limited is a wholly owned subsidiary of Cathay Pacific Airways Limited and Cathay Pacific Airways Limited manages and provides IT support services to Hong Kong Dragon Airlines Limited.

Additional Information

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Security Freeze. You have the ability to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your

name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is \$5.

For Rhode Island residents: The credit bureaus may require you to pay a fee to place, lift, or remove the security freeze.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.

Number of Rhode Island Residents Affected: Approximately 1