



## Notice of cyber security incident

Released : 19 May 2020 11:51  
RNS Number : 3627N  
easyJet PLC  
19 May 2020

19 May 2020

**easyJet plc**  
**('easyJet' or the 'Company')**

### **Notice of cyber security incident**

Following discussions with the Information Commissioner's Office ("ICO"), the Board of easyJet announces that it has been the target of an attack from a highly sophisticated source. As soon as we became aware of the attack, we took immediate steps to respond to and manage the incident and engaged leading forensic experts to investigate the issue. We also notified the National Cyber Security Centre and the ICO. We have closed off this unauthorised access.

Our investigation found that the email address and travel details of approximately 9 million customers were accessed. These affected customers will be contacted in the next few days. If you are not contacted then your information has not been accessed. Other than as referenced in the following paragraph, passport details and credit card details of these customers were not accessed.

Our forensic investigation found that, for a very small subset of customers (2,208), credit card details were accessed. Action has already been taken to contact all of these customers and they have been offered support.

We take issues of security extremely seriously and continue to invest to further enhance our security environment.

There is no evidence that any personal information of any nature has been misused, however, on the recommendation of the ICO, we are communicating with the approximately 9 million customers whose travel details were accessed to advise them of protective steps to minimise any risk of potential phishing. We are advising customers to continue to be alert as they would normally be, especially should they receive any unsolicited communications. We also advise customers to be cautious of any communications purporting to come from easyJet or easyJet Holidays.

We're sorry that this has happened, and we would like to reassure customers that we take the safety and security of their information very seriously.

easyJet is in the process of contacting the relevant customers directly and affected customers will be notified no later than 26<sup>th</sup> of May.

Customers can also find further advice at [www.actionfraud.police.co.uk](http://www.actionfraud.police.co.uk)

easyJet Chief Executive Officer Johan Lundgren said:

"We take the cyber security of our systems very seriously and have robust security measures in place to protect our customers' personal information.

However, this is an evolving threat as cyber attackers get ever more sophisticated.

"Since we became aware of the incident, it has become clear that owing to COVID-19 there is heightened concern about personal data being used for online scams. As a result, and on the recommendation of the ICO, we are contacting those customers whose travel information was accessed and we are advising them to be extra vigilant, particularly if they receive unsolicited communications.

"Every business must continue to stay agile to stay ahead of the threat. We will continue to invest in protecting our customers, our systems, and our data.

"We would like to apologise to those customers who have been affected by this incident."

This release contains inside information.

**For further details please contact easyJet plc:**

Institutional investors and analysts:

Michael Barker 939	Investor Relations	+44 (0)7985 890
-----------------------	--------------------	-----------------

Holly Grainger 913	Investor Relations	+44 (0)7583 101
-----------------------	--------------------	-----------------

Media:

FleishmanHillard 889		+44 (0)2039 255
-------------------------	--	-----------------

LEI: 2138001S47XKWIB7TH90

This information is provided by RNS, the news service of the London Stock Exchange. RNS is approved by the Financial Conduct Authority to act as a Primary Information Provider in the United Kingdom. Terms and conditions relating to the use and distribution of this information may apply. For further information, please contact [rns@lseg.com](mailto:rns@lseg.com) or visit [www.rns.com](http://www.rns.com).

END

MSCFLFSIEDIALII