FAO: Matthew Roberts
National Officer for Aviation
GMB Union
Mary Turner House
22 Stephenson Way
Euston
London
NW1 2HD

By Email: Matthew.Roberts@gmb.org.uk

22 June 2023

Dear Mr Roberts

Zellis Cyber Incident ("Incident")

I write further to my email of 16 June 2023.

By way of background, Zellis provides payroll support services to hundreds of companies in the UK, including BA. We have been working intensively with Zellis to understand what happened, including the extent of the impact on our colleagues' personal information as a result of the Incident.

In response to your questions:

1. *When exactly was the breach identified and how soon after the discovery were our members notified?*

   Upon learning of the Incident during late afternoon on Friday 2 June 2023, teams worked through the weekend to analyse the affected files to ascertain which colleagues and what data had been affected.

   Affected colleagues were informed on Monday 5 June from 9.30 am, together with Q&As and notified that Experian credit monitoring services would be made available. The Experian codes were then made available on the morning of Tuesday 6 June. We continue to update Q&As and circulate colleague communications with further information as and when we receive it.

2. *Why was the vulnerability not identified sooner?*

The Incident occurred because of a new and previously unknown vulnerability in the MOVEit file transfer tool used by Zellis (the tool is used by organisations globally including UK and US government bodies).

Once the vulnerability was identified, immediate steps were taken by Zellis to contain it and investigations began into its potential impact. Connectivity to the Zellis server which used the MOVEit tool has not been restored at this time.

3. *What have the investigations found so far and will there be full transparency to our members?*

   The compromised files were exfiltrated from an encrypted server. The way the malicious actor exfiltrated the files was by exploiting an unknown zero-day vulnerability in Progress' MOVEit Transfer software, that allowed the bad actor to bypass the encryption by posing as an authenticated user with administrator access. Forensic analysis by an external expert security company on behalf of Zellis has confirmed no other malicious activity outside of this single isolated instance.

   We and Zellis have informed the Information Commissioner's Office ("ICO"), the UK National Cyber Security Centre ("NCSC") and the National Crime Agency ("NCA") of the Incident. We shall continue to cooperate with those authorities in order that they can investigate and continue to inform affected individuals of material developments as we become aware of them.

   On 14 June, Clop started to share the names of organisations on their website for whom they claim to be holding data. Neither BA nor Zellis were named. We are continuing to track this and also monitor the dark web for the exfiltrated files. We have so far identified no evidence that the files have been posted.

4. *Would you undertake a review of the use of outsourcing and external suppliers in the light of this event with a view to insourcing?*

   We do not outsource payroll. We have an internal team of 22 colleagues in the People directorate. The agreement with Zellis relates to the payroll system.

5. *What due diligence was undertaken on this contractor and what data sharing agreement was in place between the employer and the contractor?*

   Zellis is a leading provider of payroll services in the UK. Comprehensive contractual protections around data protection were in place and Zellis has appropriate accreditations from a cyber security perspective. The cause of the

incident was a zero-day vulnerability in the MOVEit file transfer service as set out above.

6. *Will the company issue a full apology to all of our members, many of whom are distressed by this breach?*

   Our number one priority is providing support to our employees and protecting their data. Colleagues have been assured that we are taking the Incident incredibly seriously and will continue to keep them updated.

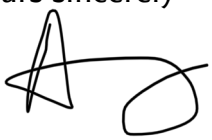
   In the meantime, the Experian service provided to employees allows access to a web monitoring service based on personal details that employees ask to be monitored (details have not been provided to Experian by BA). We recommended affected employees use the Experian service.

7. *Will be there be a wider review of all data holding and processes within BA to ensure maximum trust and security?*

   Our processes remain under continual review and all learnings from the Incident will be taken into consideration.

Finally, with respect to your query in the final paragraph of your letter, given the facts of the incident as they are currently understood, there is no indication that there has been any breach of data protection laws and therefore no fine would be anticipated.

Yours sincerely



Andrew Fleming
General Counsel & Company Secretary
British Airways Plc