CONFIDENTIAL

The Aviator Hotel (Farnborough) Limited
Personal Data Breach Assessment
Date: 21st April 2026

---

1. Summary

Internal Reference	
Office / Location	The Aviator Hotel (Farnborough) Limited, the parent company for which is Farnborough Airport (Holdings) Limited
Background	The Aviator Hotel uses the reservation platform, Rezlynx (Guestline), for guest bookings.
Brief summary of the breach	The login details of the Head Server with the Food & Beverage team were used by an unauthorised person unknown to gain access to Rezlynx. Whilst MFA is in place, for reasons presently unknown, this did not prevent the attack. As a result, the personal data of guests that had reservations between the period of March 2026 to September 2027 were accessed.
Date and time the Aviator became aware of the breach	8.39pm on Monday 23rd March 2026 The Aviator was notified by Guestline Support.
Number of data subjects affected	The overall number of data subjects who have been affected is 1,428. However, only one (1) of the affected data subjects reside in New Hampshire.
Nature of the breach (sensitivity and volume of personal data)	The breach was an unauthorised access to the booking platform, , using login credentials that were illegally obtained and as a result, an unauthorised user accessed the booking summaries of some of the Aviator's hotel guests.
Categories of personal data	The following personal data relating to guests has been compromised (noting that not all of the below data types is present for all bookings): Name, email address, phone number, date of arrival, date of departure, booking reference number, the name of the guests employer (if this information was inserted into their guest profile because, for example, their employer paid) and the cost of the accommodation. The full payment card details are NOT stored in the system and could not, therefore, be accessed.
Root cause of this breach	Malicious attack by a person unknown and the investigation is still on-going.

Severity of consequences for data subjects	We have since been advised by some of the data subjects affect that the malicious actor has used the email addresses obtained to send phishing emails for fraudulent purposes. In particular, they have sent emails to some of the data subjects affected asking them to confirm their booking by clicking on a link. The emails are made to look as if they have come from the Aviator and they press the recipients to act within 24 hours otherwise their booking will be released. Nobody has clicked on the links as far as we know. However, we are concerned that the link may take the user to a payment screen where they will be invited to submit credit / bank card details and make a payment and/or release malicious code. The malicious actor, potentially, had access to the data for up to 24 hours because this is how long the cookies last for this platform. Whilst the login details were changed within 23 minutes, this would have only prevented new logins and access to other pages within the system and not the page or pages that the malicious actor was viewing at the time.
Any special characteristics of the data subjects	None other than that mentioned above.
Mitigation steps taken	1. Immediately that the incident came to light the matter was reported internally to management and IT. 2. The compromised account was secured by changing the login credentials and, as a precautionary measure, all other users of at the Aviator also had their login credentials changed. 3. The DPO was notified and their advice was taken. 4. A full investigation began and a crisis group was formed 5. We have notified the insurers for the Aviator. 6. We have notified the National Crime Agency in the UK.

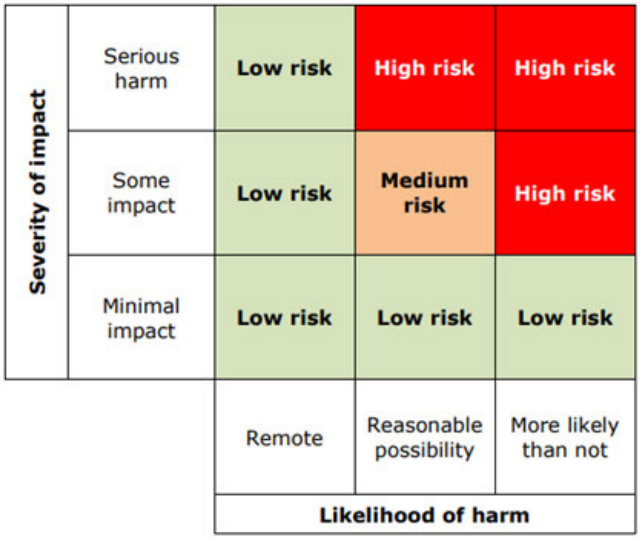
	7. We have also notified the data subjects affected, apologised and provided advice on how they can take steps to protect themselves, as necessary.
Corrective actions recommended	Whilst the investigation is ongoing, the following corrective actions have been identified so far and will be implemented urgently, if they have not already: • was found to have outdated software. • have had software updates to latest versions. • that was used to log in into was found to present an unusual screen and this device has now been wiped and will be securely destroyed. • Measures will be implemented so that updates are regularly installed and cannot be rejected. • The Aviator will now have a full cyber security review. We are working closely with our service providers, our IT experts and our DPO to ascertain as much information as possible and we will implement any additional technical and organisational measures they consider appropriate in order to protect the personal data we are responsible for and ensure our systems are robust.
Has the person responsible for the breach had data protection training in the last two years?	Whilst the investigation is ongoing and we have not yet established who was responsible for the breach, we can confirm that the employee whose login credentials were illegally used to access the booking platform has had regular training in data protection and security awareness, including numerous sessions on particular topics within this space over the last two years.
Assessed level of risk	High
Completed by (Name & Role)	The Aviator in consultation with the external DPO

2. Risk Assessment

The incident may have affected up to 1,428 data subjects overall, although only one (1) in New Hampshire. The data accessed contains their contact details and details about their reservations at the Aviator,(although not all categories for all data subjects) which could be mis-used to cause financial or other harm to the individuals. For example, as mentioned above, some of the email addresses have already been used to send phishing emails to some of the data subjects affected. The emails urge the recipients to click on a link within the email to confirm their booking. We do not know what will happen if anyone does click on a link as we have had no reports that anyone has to date. However, we are concerned that clicking on the link could release malicious code or send the user to a payment screen where the malicious actor will attempt to fraudulently extract funds. The "severity of impact" is, therefore, assessed as "serious harm".

As the incident was a malicious attack, it is reasonable to assume that the data will be used for malicious intent and we, therefore, assess the "likelihood of harm" to be "more likely than not".

We have assessed the risks by reference to the following risk matrix:



3. Recommendation

As the risk to the data subjects is assessed as high, we will report this breach to the relevant supervisory authorities and add it to our Personal Data Breach Register. We also propose the corrective actions listed in the Summary section be applied as a matter of urgency and additional measures will also be implemented, as necessary. We will continue to investigate the matter and update the supervisory authorities with developments, if appropriate.

4. Sign-Off

Recommendation Accepted: YES

Name: Sandra May

Role: Principal Data Protection Consultant, Evalian Limited – DPO for the Aviator

Date: 21st April 2026

Email sent to data subjects affected on or about Friday 27th March 2026

Dear Guest,

We have recently been informed by one of our platform providers of a security issue that has resulted in some guest contact details (such as email addresses) and reservation information (such as booking reference numbers) being accessed by an unknown third party without authorisation. However, we can confirm that no payment card or postal address details have been accessed.

As a precaution, we would advise you to be vigilant in case the third party sends you an email purporting to be from the Aviator or a booking-related platform, asking you to verify your reservation or requesting your payment card details. Please note that these emails would not have been sent by us.

If you do receive such an email, please do not click on any links or provide any personal or payment information. If you do, we recommend that you contact your payment card provider immediately.

We are currently investigating the cause of the incident however we can confirm that we have contained the incident and implemented additional technical and organisation measures to safeguard your information. As such, there is no ongoing risk. We will also now undergo a complete cyber security review with a view to strengthening our systems further.

If you have any questions, please contact us on 01252 555 890.

Kind regards,

Aviator Hampshire