Dear Customer,

Please be advised that one of our suppliers, Accelya, who host the BSPLink on our behalf, has been the subject of a ransomware attack. Please find attached a formal notification from IATA to you in relation to this security incident and which provides further information that we are aware of at this time.

We are working with Accelya to ascertain further details and information and will be in contact as further information becomes available.

Yours sincerely,
Muhammad Ali Albakri
IATA SVP
Financial Settlement and Distribution Services

CONTROLLER/CUSTOMER NOTIFICATION

We are writing to inform you that we have become aware of a ransomware (AlphV Blackcat) attack which has affected our service provider Accelya (data processing centre based in Madrid) (https://w3.accelya.com/about-us/). The attack on Accelya has affected the operation of our new BSPLink and as such Accelya reverted to the classic BSPLink to ensure continued operations of the system.

At this point in time, it's unclear exactly what BSP data or if any replicated data used by Accelya in its own solution(s) has been compromised or leaked because of the security incident. We are therefore currently unable to confirm what (if any) categories of personal data and approximate number and records of data have been affected.

Further details of the incident

Regrettably the information we have been provided by Accelya has been extremely limited, notwithstanding attempts to press them for further details.

We understand that on 3 August 2022 Accelya identified that they were the subject of a ransomware attack. Accelya informed us on 5 August 2022 of service delivery difficulties, and that these were due to the ransomware attack that had occurred on the 3 August 2022 and advised us on the 16 August 2022 the nature and identity of the ransomware. We understand that the attack has affected the primary and separate backup for the new BSPLink that Accelya operates.

At this time Accelya have said they cannot confirm whether personal data processed for you within the BSP systems has been directly impacted within the attack, and they are estimating it will take them at least 2-3 weeks to confirm the position. They have engaged a third-party forensic investigation firm to assist them.

Why are you notifying us now?

We are taking the decision to notify you now because we have separately become aware that some data from the attack has been released into the public domain. In addition, we have independent sources that have provided us with a clear indication that certain BSP systems data has being leaked into the public domain and we are currently analyzing this to determine the potential extent of this exfiltration and publication. We will further update you if we become aware of other BSP system data being exfiltrated, compromised or released into the public domain, including any personal data.

We wanted to bring this to your attention without undue delay and appreciate that you will want to understand the impact on personal data at the earliest opportunity as you in turn consider notifications and reporting requirements.

Next steps

To facilitate continuity of service for our customers traffic, we will continue to reroute through classic BSPLink, until further notice.

There is no evidence of the attacker group having used access gained at Accelya to access IATA systems, but we continue to undertake due diligence to check this. It would be prudent for you to undertake appropriate security checks in the light of this incident. We have requested from Accelya precise IOCs (Indicators of Compromise) in order to give to your security team to allow you to detect and block any similar attack from the hackers. Once we have received this information, we will pass this on to you.

We will continue to press Accelya for further information, evidence and supporting documents relating to the data security incident in order to assist the assessment of whether this security incident would trigger any reporting or notification obligations. We will update you as further information becomes available.

In the meantime, please contact our Customer Services team if you have any questions relating to your use of BSPLink or this security incident.