TRAVEL AGENCY COMMISSIONER - AREA 1
Deputy Commissioner for Area 2
VERÓNICA PACHECO-SANFUENTES
110 – 3083 West 4th Avenue
Vancouver, British Columbia V6K 1R5
CANADA

DECISION – September 27th, 2018

In the matter of:

International Loisirs et Services S.A. ("ILS")
IATA Code # 54-2 2118
94 Rue Jean Jaurès
Casablanca, 20000
Maroc
Represented by its Managing Director, Mr. Mohamed Amine Filali
The Agent

vs.

International Air Transport Association **("IATA")**
Global Distribution Centre
Torre Europa
Paseo de la Castellana, 95
28046 Madrid, Spain
Represented by the Assistant Accreditation Manager, Mr. Francesco Chiavon
The Respondent

I. THE CASE

The Agent sought this Office's intervention in light of its sudden suspension from the BSP system. The Respondent executed the suspension based on what, at first sight, was a significant sales' increase reflected on the Agent's BSP Sales Report for the month of July.

A day after having suspended the Agent, the Respondent was informed by the GDS (Amadeus) that such abnormal increase in the Agent's Sales Report had been caused by an electronic hacking that had occurred on Amadeus own system during the night between the 21st and 22nd of July 2018 (Saturday and Sunday) affecting the Agent, yet where the Agent had neither participation nor knowledge about.

The Responded requested from the Agent the immediate settlement of amounts due (even of those amounts for which Remittance Date has not arrived) and the submission of a bank guarantee ("BG"), as a reinstatement requirement.

The Agent is challenging all of the above and the relief sought is its prompt reinstatement into the BSP system and IATA's cooperation to solve this fraudulent situation in a commercially oriented fashion, rather than punishing the Agent for having committed no wrong.

II. BACKGROUND

The facts and legal grounds, as they have been pleaded by the Parties and substantiated by evidence, are as follow:

- The Agent has been an Accredited Agent for 30 years, never before being faced to a suspended from BSP situation or any type of default;

- GDS-Morocco (Amadeus) was the subject of an electronic hacking affecting their computerized ticketing system. As a ripple effect, this GDS hacking impacted accredited agents in the Moroccan market, the Agent to this review procedure being one of them;

- The GDS/Amadeus hacking occurred during a Saturday night (started at 21H07min–local time) and a Sunday night (21-22 July 2018), impacting the Agent at a time when the Agent's office was closed for the weekend, the staff in charge of ticketing had already logged out from Amadeus system; and after having turned off, as a precautionary measure, the internet connectivity altogether;

- More than 200 tickets were issued during few late hours of those 2 nights;

- In the contract signed between the Agent and Amadeus is stated the Agent's business hours. Amadeus has the Agent's telephone contacts for after-hour's emergency situations. However, none of these telephone numbers were used by Amadeus when the hacking occurred in order to give timely alert to the Agent;

- The only contact that *Amadeus Security Service* made with the Agent was through three emails sent at 23h15min and at 23h16mn (local time), when the Agent's premises were closed (it was the middle of the night during a weekend) from a noreply@Amadeus.com sender email, portraying to give the Agent an access code in order to get into Amadeus' server;

- No evidence was provided showing that the Agent had indeed used such codes; the contrary was actually established. The Agent never used those codes nor attempted to access Amadeus from its computers during those weekend hours;

- The Agent's login ID number was not used in any of the fraudulent tickets;

- Days after the events (on July 31), Amadeus alerted the Moroccan community of Accredited Agents about these fake emails sent from noreply@Amadeus.com,

ensuring Agents that there was no need for any activation of any code in order to enter into Amadeus system, that Amadeus system was automatically updated, hence, no need for any Agent's actions. Amadeus encouraged Agents to discard these fraudulent messages and to report them as soon as possible;

- On Monday July 23rd the Agent reported the incident to Casablanca Police Department, Cyber Criminality Section (file No. 1722 / 2018). The Responded was duly informed too.

- The fraudulent tickets represented approximately between 70% - 75% of the total BSP Sales Report;

- Once the GDS computer hack was detected and the Agent was informed about it by the GDS, the Agent immediately contacted the concerned Airlines and tried to get the tickets involved cancelled and refunded by the respective carriers;

- *Air France* was fully cooperative and, as soon as presented with all the evidence of the case by the Agent, it cancelled, *motu propio*, all the fraudulently issued tickets. It also addressed the Respondent requesting them to deduct the total amount of *Air France* tickets from the Agent's BSP Sales Report;

- *Air Maroc*, from where the vast majority of fraudulent tickets were issued:

    - after having insisted on the Respondent to instruct the GDS to activate the Agent only to allow it to process all pending refunds in order to reduce the Agent's actual debt, which after some reluctance, the Respondent did;
    - it also reached out to the Agent and is supporting it. They have reached a bilateral agreement tackling this situation;

- The refunds approved by *Air Maroc* and processed through BSP, done the 26th and 27th of July, correspond a total of MAD 915,264.15 (US$ 97,512). The total sales made during that period (from 1 to 23 July 2018) were MAD 3,413,573.41 (US$ 363,681);

- On August 6th, the Respondent suspended the Agent, placing it «*under review*», invoking Resolution 818g, Attachment "A", s. 1.7.8.1, ss. (viii);

- On August 27th, since the Agent could not pay all the amounts requested by the Respondent (*id est*, amounts owed to the BSP in addition to the sales not yet due), it was declared in default. The amounts claimed by the Respondent are:

    - Total BSP Sales Report for the period 20180701M: MAD 2,498,641.01 (US$ 266,205)
    - Total disputed (post billing dispute): MAD 431,928.17 (US$ 46,017.50)
    - Total amount due to BSP, still unpaid: MAD 2,066,712.84 (USD 217,601.63)

It is well known in the industry, that each ticket has a history, where all the details of a ticket can be found and where each ticket can be fully traced. This "history" is held by the GDS (Amadeus in this case), yet it has refused to communicate it or to show it to the Agent.

The Agent recognises being responsible for **the security and safeguard of its premises and electronic ticketing system during business hours**, as clearly established in the contract signed between Amadeus and the Agent, as well as in the applicable Resolutions. Nonetheless, it contests having any responsibility for what can happen during weekends or outside business hours, outside its premises, when the system is under the sole control and monitoring of Amadeus, and when the Agent's staff had properly logged out and even turned off all internet connectivity. The Agent invokes *force majeure*.

The Respondent claims that the Agent is responsible, as per Resolution 818g, ss. 2.1.11 and 2.1.13, for the security and protection of electronic ticketing and argues having followed correct procedure, as per Resolution 818g, Attachment "A", s. 1.7.8.1, ss. (viii).

III. ORAL HEARING

In the opinion of this Commissioner, according to Resolution 820e, s. 2.3, and without jeopardizing any Parties' rights, an oral hearing was not deemed necessary and the Parties, after having been consulted, did not object this conclusion. Ample opportunity was given to them to present their submissions and evidence accordingly. They both made good use of their right. Therefore, this decision is based on that written documentation only.

IV. CONSIDERATIONS

Looking at how the case has been pleaded by the Parties and the evidence provided in support of their submissions, I see the matters to be reviewed as follow:

(1) Whether or not IATA followed proper procedure when suspending the Agent in accordance with Resolution 818g, Attachment "A", s. 1.7.8.1, ss. (viii);

(2) What obligations/rules did the Agent infringe?

(3) Whether or not, pursuant s. 13.8 of Resolution 818g, the Agent is responsible for the computer hacking that occurred in the GDS, resulting in the issuance of fraudulent tickets and the consequences derived from such ticketing, or, if the situation amounts to *force majeure* and, hence, the delay/failure to comply shall be deemed excused or exonerated.

(1) <u>Proper procedure when suspending the Agent</u>

The first point that I will refer to is about a procedural aspect of the Respondent's actions.

Based on the evidence on file, in/or about the time of suspension the Respondent only had *written information* about the Agent's sudden spike on sales and about the electronic hacking that had occurred on the GDS system. In other words, the Respondent, at that time, was facing a scenario where the security of tickets' issuance seemed to have been compromised. In this context, the Respondent was mandated, as per s. 2.1.11 of Resolution 818g, to follow the provisions stated in s. 5. Consequently, the procedure mandated in s. 5.5.2 should have been applied and:

(i) An invitation for an explanation should have been sent to the Agent; and,
(ii) If no explanation would have been received during the next 10 working days of its request, or, if the explanation was unsatisfactory, the Respondent had to refer the matter to this Office for review and action.

In case such procedure would not have been deemed expedite enough, given the seriousness of the situation, the Respondent had the discretion, based on the *written information* that it had at hand at that time, to apply the procedure prescribed in s. 1.8 of Resolution 818g, Attachment "A" referred to as *Prejudiced Collection of Funds* and immediately suspend the Agent from the BSP and request, right after that, a review from this Office, as per ss. 1.8.2.

The grounds for my conclusion are based on the following facts:

(a) The procedure applied by the Respondent, set out in Resolution 818g, Attachment "A", s. 1.7.8.1, ss. (viii) presupposes the existence of <<*an audit or other investigation*>>, and none of these situations were present in this case or were they proven by the Respondent. Neither an *audit* nor an *investigation* had been undertaken by the Respondent into the Agent's system or on its business. The Respondent, at the time of the suspension, only had in front of it a BSP Sales Report (a *written information*) indicating a considerable increase on the Agent's sales, compared to its "usual" sales' volume. And a day after, the Respondent got more *written information*, this time from the GDS, who expressly admitted having been the subject of an electronic hacking that affected their system, at late night hours, impacting the Agent's reflected sales, amongst other Agents in the region.

(b) The second requirement established in s. 1.7.8.1(viii) is about a <<*failure to prevent the unauthorised or fraudulent use of computer-generated document…*>>. The evidence shows an express admission from the GDS provider regarding an electronic hacking occurring on their end, specifically at a time when the Agent's system was not operative. There is no proof on file that incriminates the Agent in respect to any *failure* preventing an unauthorised or fraudulent use of computer generated documents. On the contrary, not only the national carrier but a major international carrier both have expressly exonerated the Agent, based on the evidence that was part of this review procedure, from any wrongdoing and

have understood that the Agent was in fact a *bona fide* victim of fraudulent behaviour from a third criminal party.

It is important to note that **bad faith, such as fraud, cannot be presumed**; it has to be proven. This statement takes us to the next question to be solve in this review:

(2) What obligations/rules did the Agent infringe?

The Respondent did not prove any failure from the Agent's side in respect to its obligations towards the '*security*' of its systems and premises, as stated in Resolution 818g, ss. 2.1.11 and 2.1.13.

Conversely, the Respondent did have the admission of the GDS in regards of having been the subject of a hacking on their system, directly affecting the Agent. It is not for the Agent to prove its innocence, which in any event, the Agent has done, but it is **the Respondent's burden to prove the Agent's involvement in any fraudulent activity** or any failure to comply with its obligations as an Accredited Agent. The record shows that the Respondent did not discharge its duty.

Looking close at the *supra* mentioned ss. 2.1.11 and 13, an Agent has the obligation to:

> *<<… undertake to provide sufficient protection for **its** business, premises and systems used for the issuance of STD's in accordance with the provisions detailed in Section 5 of this Resolution>>*
>
> Furthermore, Agents are *<<recommended to take all necessary precautions to protect **its** business applications>>*.

The evidence on file shows the Agent's compliance with its undertaking to provide sufficient protection to ***its*** business, premises and systems used for the issuance of STDs and it took the necessary precautions to achieve this on its end. In fact, the premises were closed, no burglary, or robbery or any type of trespass occurred on the Agent's premises; the ticketing access to Amadeus had been logged out by the Agent's staff; internet connectivity had been disconnected for the weekend, so no online ***breach of security facilitating the possibility of fraudulent*** ticketing. The Respondent rebutted none of these facts.

The fraudulent situation, the non-compliance with security standards did not occur on the Agent's side. The violation of the electronic system did not occur on the Agent's premises nor was it caused by the Agent's staff. The GDS has expressly admitted that their system had been hacked causing the fraudulent tickets to be issued. This is the evidence on file, which was submitted actually by both Parties.

Section 5, particularly s. 5.1, creates the Agent's Duty of Care towards the issuance of STD in the following terms:

<<An Accredited Agent is duty bound to take all reasonable care and precautions to secure Standard Traffic Documents ***assigned to it*** *and to protect them from unauthorised or improper issuance or post-issuance tampering* ***whilst in its custody***>> (emphasis mine)

It is essential to read this provision quite carefully; it merits some comments:

(i) It establishes the duties that an Agent has in regards to securing *Standard Traffic Documents ("STDs");* however, there are no STDs anymore. STDs referred to physical tickets or actually to tickets' stocks that were given to Agents and they were responsible for their safety and custody. Nowadays are electronic times, no STDs/physical tickets "*are assigned*" to any Agent anymore, as the rule describes;

(ii) Even if doing the exercise of adapting the wording to our modern era, and considering that the Agent had the obligation to protect the system from where the electronic tickets are issued, as explained *supra*, it did discharge its legal obligations, it did take the precautionary measures that it could take on ***its*** end. It was not its system the one who failed, the one who was vandalised/hacked; as the evidence clearly demonstrated the **security failure occurred at the GDS' premises**, it was the GDS system the one who was hacked;

(iii) No Agent has any control over the security safeguards that a GDS undertakes or not to protect their systems. Agents are simple users of the system under the terms and conditions established by the GDS providers and by IATA;

(iv) Conclusively, the rules under analysis do not create an obligation for an Agent to protect '*others*' business, '*others*' premises nor '*others*' systems – but rather a duty of care for "***its***" own (as emphasised *supra*, when the rule is quoted) and it is responsible for that.

Based on those facts, I find that the Agent did not breach its duty of care, as referred to in s. 5.1 of Resolution 818g. The evidence in front of me does not demonstrate the breach of any contractual obligation by the Agent, as prescribed in the PACONF Resolutions applicable to its Passenger Sales Agency Agreement. Therefore, since no breach was proven by the Respondent, no strict liability could be imposed against the Agent.

(3) <u>Force Majeure situation</u>

In any event, assuming that the Respondent considers that a breach of the Agent's duty of care had occurred, it is necessary to look at Resolution 818g, s. 13.8, which specifically addresses the situations where Agents *<<shall not be liable for delay or failure to*

comply>> with their obligations to the extent that such delay or failure is caused by (i) <<*… third party criminal act… beyond the reasonable control of the Agent, and (ii) is not the result of the Agent's lack of reasonable diligence ("an Excusable Delay")*>>.

After carefully reviewing the evidence on file, particularly the fact that two main carriers have, by their own initiative, accepted the evidence provided by the Agent and have expressly exonerated the Agent from any wrong in respect to these fraudulent tickets, I am satisfied that (i) the Agent was indeed the victim of a *third-party criminal act*, (ii) such event was *beyond its reasonable control*, and, (iii) it *was not the result of the Agent's lack of reasonable diligence*; therefore, I deem that the Agent should be excused from the situation in which it has been immersed into.

Furthermore, the evidence shows that as soon as made aware of the electronic hacking, the Agent took immediate steps in order to minimize its losses and to be an active participant of a potential solution to a damaging situation for all the parties involved. It immediately reported the incident to the police authorities, contacted the Airlines concerned, reached out to the GDS and had constant contact with the Respondent.

Considering that the Agent was a victim not the perpetrator of a third-party criminal act, following this Commissioner's interpretation of *force majeure*, pursuant the above-mentioned rule, the Agent should be excused from any obligation to pay any of those fraudulent tickets, as it was excused by *Air France* (as referred to *supra*).

Important note for the Respondent:

Since IATA's main mission is to protect BSP Airlines' funds;

Considering that those funds are the result of tickets sold by IATA Accredited Agents that operate in a given market, using the electronic platform provided by their local GDS and processed through the BSP;

I deem important for IATA to be aware of certain details that surfaced in this review procedure affecting the GDS providers, at least in the Moroccan market (and I would presume, judging from the news that have been more and more often referred to by the international press, that this is not an isolated case nor a "Moroccan situation").

Those details that I am taking the liberty to bring to IATA's attention are the following (some of them *verbatim* from the Agent's submissions and evidence, not contradicted by the Respondent):

- Amadeus' system was accessible during all times of the day; no special security measures were in place on their system for "after hours" ticketing. This proved to be problematic, creating a weak spot for hackers to take advantage of;
- Upon the Agent's advice, in an attempt to tackle this situation, Amadeus has started to close its system to all travel agents in Morocco as of 19h30min during week-days and during the entire weekend;

- Furthermore, fully aware of their system's weakness and failure to prevent this type of electronic fraud, Amadeus has launched a pilot project demanding a validation code, by SMS, as the Banks do;
- The Director of Amadeus Casablanca, Agent's *dixit*, has indicated that the amount of fraudulent tickets affecting the Agent was derisory and that they could afford it easily; but they were afraid that by doing so they would be creating a precedent, since they are affected by those kinds of electronic hacking almost every day somewhere in the world;
- Apparently, several former "black hackers" converted into "white hackers" have proved the technical failures of most of GDS's ticketing systems given their manifested security insufficiencies. As it is a well-known fact, many Airlines have been heavily affected by this phenomenon.

V. DECISION

Based on the referred arguments, evidence and applicable rules, it is hereby decided as follows:

- The Agent has fulfilled its duty of care, as per s. 5.1 of Resolution 818g; therefore, no strict liability can be applied against it (s. 5.2 of same Resolution);

- In any event, the Agent is, as per Resolution 818g s. 13.8, **exonerated** from any failure or wrongdoing derived from the electronic hacking that occurred in the GDS (Amadeus) system, where he resulted affected;

- The Agent shall be **reinstated into the BSP** system as soon as it pays the amount of the July 2018 BSP Sales Report corresponding the sales effectively made by the Agent and excluding the fraudulent tickets (which, subject to the Respondent's verification, sums the total of MAD 816,829.10) (approx. US$ 87, 024,80), without having to pay any other amount nor fulfil any other reinstatement requirement;

- The BG originally requested in the Default Notice is null and void, since no wrongdoing was proven against the Agent.

This decision has immediate effect.

Decided in Vancouver, the 27th day of September 2018.

In accordance with Resolution 820e § 2.10, any Party may ask for an interpretation or correction of any error, which the Party may find relevant to this decision. The time frame for these types of requests will be 15 days after receipt of the electronic version of this document (meaning no later than October 12th, 2018).

Both Parties are also hereby advised that, unless I receive written notice from either one of you before the above mentioned date, this decision will be published in the Travel Agency Commissioner's secure web site, provided no requests for clarification, interpretation or corrections have been granted by this Commissioner, in which case the final decision will be posted right after that.

If after having asked for and obtained clarification or correction of this decision, any Party still considers aggrieved by it, as per Resolution 820e § 4, the Party has the right to seek review by Arbitration in accordance with the provisions of Resolution 824 § 14, once the above-mentioned time frame would have elapsed.