Wireless Application Service Providers' Association

# Report of the Adjudicator

| | |
|---|---|
| Complaint number | #41462 |
| Cited WASPA members | Newstor Private Limited (1874) |
| Notifiable WASPA members | n/a |
| Source of the complaint | WASPA Compliance Department |
| Complaint short description | Reasonable steps not taken to prevent fraudulent use of member's networks and systems. |
| Date complaint lodged | 2019-06-05 |
| Date of alleged breach | 2019-06-04 |
| Applicable version of the Code | v16.6 |
| Clauses of the Code cited | 4.11(a) |

| | |
|---|---|
| Related complaints considered | n/a |
| Fines imposed | Payment of R100 000 for contravention of clause 4.11(a), of which R50 000 payable immediately and R50 000 suspended for 6 months |
| Other sanctions | n/a |
| Is this report notable? | n/a |
| Summary of notability | n/a |

## Complaint

1. This complaint was lodged by the WASPA Compliance Department after tests conducted by the complainant on the Member's system on two separate occasions on the same day identified that the Member had failed and/or omitted to implement one or more of the measures set out in section 2.3 of the WASPA Fraud Detection and Mitigation Best Practice Guidelines (version 2.1).

2. The test results showed the page on the relevant domains immediately before the Network Hosted Confirmation Page did not comply with the following requirements:

    2.1 The Content Security Policy Frame-Ancestors Directive had not been implemented; and

    2.2 A ''HTTP 302'' code was presented, which meant that any security requirements that may have been set, did not render and would not work effectively.

3. The Complainant provided screenshots showing the results of the tests conducted.

4. The Complainant therefore alleges that the Member's systems remained vulnerable and were not sufficiently secured to prevent potential fraudulent attacks or activity.

5. As such, the Member is alleged to be in breach of clause 4.11(a) of the WASPA Code of Conduct.

---

## Member's response

6. The Member admitted that it had not implemented the measures set out in section 2.3 of the WASPA Fraud Detection and Mitigation Best Practice Guidelines as outlined by the Complainant, and that the relevant changes had subsequently been implemented.

---

## Sections of the Code considered

7. The complainant cited clause 4.11(a) of the WASPA Code of Conduct as the basis for their complaint.

8. Clause 4.11(a) states:

   *Members must take reasonable steps to prevent their networks and systems from being used in a fraudulent manner, including:*

   *(a) complying with WASPA's published best practices for fraud prevention;*

9. The best practices referred to in clause 4.11(a) are contained in section 2.3 of WASPA's Fraud Detection and Mitigation Best Practice Guidelines (version 2.1).

10. No further clauses were assigned by WASPA.

---

## Decision

11. I have reviewed the test results provided by the Complainant and it is evident that the Content Security Policy Frame-Ancestors Directive has not been implemented on the page immediately before the Network Confirmation Page for the relevant domains and a ‘’HTTP 302’’ code was presented.

12. The Member has admitted that it failed in this regard to implement the relevant measures set out in section 2.3 of WASPA’s Fraud Detection and Mitigation Best Practice Guidelines.

13. The Member has therefore contravened clause 4.11(a) of the WASPA Code of Conduct, and the complaint is accordingly upheld.

---

## Sanction

14. Effective fraud prevention and mitigation is clearly in the best interests of all stakeholders in the industry. Clickjacking and similar attacks pose particular concerns for members and consumers alike in the context of subscription services, where consumers continue to be subscribed to such services without their knowledge or express assent.

15. The measures prescribed in section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines are relatively easy to script and inexpensive to implement.

16. The Member failed to implement the required measures and its failure must be viewed in a serious light. An appropriate sanction must take into account the serious threat that fraud poses to the industry as a whole.

17. In mitigation, it has been noted that the Member has taken steps to implement the required protections and that no prior complaints have been lodged against the Member.

18. Based on the aforegoing, the Member is fined an amount of R100 000.00 for the contravention of clause 4.11(a), of which R50 000.00 is payable immediately and R50

000 is suspended for 6 (six) months. Should the Member’s systems be tested again and found to be non-compliant within this period, the suspended fine will become payable immediately on demand.