Wireless Application Service Providers' Association

Report of the Adjudicator

Complaint number	#41340
Cited WASPA members	Joker Mobile South Africa BH (Pty) Ltd (1836)
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	2019-05-13
Date of alleged breach	2019-04-29; 2019-04-30; 2019-05-01; 2019-05-02;
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 four separate occasions identified that the Member had failed and/or omitted to implement one of the measures set out in section 2.3 of the WASPA Fraud Detection and Mitigation Best Practice Guidelines (version 2.1).

2. All four test results showed that an ''HTTP 302'' code was presented for the page on the relevant domain used immediately before the Network Hosted Confirmation Page. This meant that any security requirements that may have been set, did not render and would not work effectively.

3. The requirements, as set out in section 2.3, were implemented earlier in the flow, however, the guidelines clearly state that a page on the domain used immediately before the Network Hosted Confirmation Page should include all the relevant HTTP headers as discussed in section 2.3, include the JavaScript as discussed in section 2.3, and be served with an HTTP 200.

4. The requirements were therefore not implemented in the correct place in the flow.

5. The Complainant provided screenshots showing the results of each test conducted.

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

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

Member's response

8. In its formal response to the complaint, 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.

9. In mitigation, the Member made certain submissions:

    9.1 It had not noticed the redirect because all its sites, landings and pre-landings go to its services to get dynamically built and then the user is redirected to that site.

    9.2 It had changed the relevant landing pages for the affected URLS and was confident that the problem would not persist. In the step where a user clicks on the landing page, they would now be redirected to a DOI system where the requirements described in clause 4.11(a) of the WASPA Code of Conduct are met.

    9.3 The traffic directed to the relevant URL's had received 4477 conversions. The Member was in the process of unsubscribing all the relevant users that might have been affected by its non-compliance. It would send logs and the exact date of service cancellation for WASPA's records.

    9.4 The problem had only risen in the CELL C network and it was looking into other ways of protecting its flows to be able to provide as much security as possible.

9.5 The Member had undergone a lot of changes in the previous 6 months in its marketing teams and some things might have slipped out of its procedure of control. Given these changes and having new people not properly trained in the requirements of the Code of Conduct and general specifics about how things work in the South African market, and it considered this to be part of a failure in its internal procedures and operating manuals. This was not stated as an excuse, but just an explanation as to why non-compliance had happened.

9.6 It has operations in over 67 MNOs and the amount of traffic, campaigns, banners, and in general marketing materials that it constantly handles, changes, activates and deactivates is substantial. Each MNO and territory also has its own specific rules and policies.

9.7 The Member has over 80 ongoing campaigns in South Africa alone. It was auditing all the relevant URL's, flows, and in general the customer journey to be 100% sure that everything is in place.

Sections of the Code considered

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

11. 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;

12. 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).

13. No further clauses were assigned by WASPA.

Decision

14. I have reviewed the test results provided by the Complainant and it is evident that the Member has failed to implement the measures set out in section 2.3 of WASPA's Fraud Detection and Mitigation Best Practice Guidelines on the page on the domain used immediately before the Network Hosted Confirmation Page, as required.

15. The Member has admitted that it failed to do so.

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

Sanction

17. 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.

18. 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.

19. I have taken into account the submissions made by the Member in mitigation but these submissions do not detract from the seriousness of its non-compliance.

20. An appropriate sanction must take into account the serious threat that fraud poses to the industry as a whole.

21. Based on the information provided Member regarding the number of conversions for the affected URL's, a large number of users could have been potentially harmed by the vulnerability of the Member's systems.

22. It was however duly noted that no prior complaints have been lodged against the Member.

23. 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.

24. 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.