Wireless Application Service Providers' Association

Report of the Adjudicator

Complaint number	#39889
Cited WASPA members	Mobile World AG (1543)
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	2018-08-13
Date of alleged breach	2018-07-09; 2018-07-15; 2018-07-16; 2018-07-20; 2018-07-21;
Applicable version of the Code	v15.5
Clauses of the Code cited	4.11(a)

Related complaints considered	n/a
Fines imposed	R100 000 for contravention of clause 4.11(a), with 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 seven separate tests were conducted by the complainant on the Member's system on different days. The test results 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. Each test result showed that the page on the domain name used immediately before the network hosted confirmation page was non-compliant for the following reasons:

   2.1 No Content Security Policy Frame-Ancestors Directive set as 'none';

   2.2 No X-Frame-Options Response Headers set as 'deny'.

3. The complainant provided logs setting out the results of each test.

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. In its response to the formal complaint, the Member did not dispute the test results and that it had not complied with the requirements of clause 4.11(a) of the WASPA Code of Conduct, read together with section 2.3 of the WASPA Fraud Detection and Mitigation Best Practice Guidelines.

7. The Member, however, did state that in order to remedy the breach, the Member had organized a team of leading technical experts in the field to check all technical infrastructure and implement improvements.

8. The following steps were taken by the Member to further secure its systems:

    8.1 All relevant headers were included on all the pages served by its web server;

    8.2 JavaScript code was added to all the pages hosted on its server that were part of the landing page subscription flow;

    8.3 The code overrides the page content if it detects that the page is loaded in a <frame> or <iframe>; and

    8.4 It had checked that the page immediately before redirecting to the network subscription page responds with the correct headers and status code HTTP 200.

9. The Member confirmed that these changes had been applied to all the landing pages that were noted in the complaint and also on each of its other campaigns.

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 document (v2.1).

13. No further clauses were assigned by WASPA.

Decision

14. The incidence of fraudulent attacks and activities on the networks and systems of mobile service providers in South Africa and worldwide has become a major concern, not only for WASPA members but for all stakeholders in the industry.

15. In response to these threats and in line with its mandate to ensure that consumers can use mobile services with confidence, WASPA amended its Code of Conduct by introducing a positive obligation on its members (in terms of clause 4.11) to take *reasonable* steps to prevent their networks and systems from being used in a fraudulent manner.

16. Following due consultation, consensus was reached between the members of WASPA on what would constitute *reasonable steps* and certain prescribed protocols, standards and measures were adopted as best practice for the industry.

17. These best practice measures were published in the Fraud Detection and Mitigation Best Practice Guidelines (version 2.1), which was accepted by and is currently binding on all WASPA members.

18. Section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines sets out three different header and scripting protocols and standards to be implemented by members to prevent or mitigate against user interface redress attacks (including ''clickjacking'' and SOP bypassing), namely:

18.1 the Content Security Policy (CSP) standard created by the Worldwide Web Consortium;

18.2 the X-Frame-Options Response Header directive; and

18.3 Legacy Browser Exploit Protection.

19. Section 2.3 expressly stipulates that the prescribed measures must be adopted together, and if they are not implemented together, a member's system would still be vulnerable to attack.

20. Section 2.3 also expressly stipulates that the prescribed measures must be implemented on the last rendered page on the relevant domain used immediately before the network confirmation page.

21. I have examined the logs provided by the complainant from each of the tests conducted on the Member's system and I am satisfied that the Member has not implemented the required measures in terms of section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines.

22. The Member has also admitted that it had not implemented the security measures required in terms of section 2.3.

23. Based on the aforegoing, I am satisfied that the Member has failed and/or omitted to take reasonable steps to prevent its networks and systems from being used in a fraudulent manner as required by clause 4.11(a) of the WASPA Code of Conduct.

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

Sanction

25. 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.

26. The measures prescribed in section 2.3 of Fraud Detection and Mitigation Best Practice Guidelines (version 2.1) are relatively easy to script and inexpensive to implement.

27. The failure of a member to comply with WASPA's published best practices must, therefore, be viewed in a serious light, and an appropriate sanction must take into account the serious threat that fraud poses to the industry as a whole.

28. I have taken due notice of the fact that this is the Member's first offence with regard to a breach of clause 4.11 and that it has taken steps to remedy its breach.

29. Based on the aforegoing, the member is fined an amount of R100 000.00, of which R50 000 is payable immediately and a further R50 000 is suspended for 6 (six) months.

30. 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.