Wireless Application Service Providers' Association

Report of the Adjudicator

Complaint number	#39887
Cited WASPA members	Buongiorno South Africa (0002)
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	2018-07-16
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 two separate tests were conducted by the complainant on the Member's system on the same day. 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. Both test results 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 Content Security Policy Frame-Ancestors Directive not set as 'none';

    2.2 X-Frame-Options Response Headers not set as 'deny'; and

    2.3 A 302 code was presented, which means that any security requirements that may have been set, did not render and would not work effectively.

3. The complainant provided logs setting out the results of both tests.

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 complaint, the Member avers that it had taken reasonable steps to secure its networks and systems in compliance with clause 4.11(a) of the WASPA Code of Conduct and that the requirements in section 2.3 of the WASPA Fraud Detection and Mitigation Best Practice Guidelines had been followed.

7. In particular, the Member avers that the required security measures were included on a page rendered immediately before the network hosted confirmation page.

8. The Member alleges that the last page rendered before the network hosted confirmation page is hosted at the domain – bos.buongiorno.com. This page was not visible to users and was used by the Member as a backend measure in its subscription flow for user recognition before the user was redirected to the network hosted confirmation page.

9. The Member alleges that this ''ghost page'' contained the required JavaScript and rendered the required HTTP 200 – OK header.

10. The Member advised further that when the subscription flow is initiated, if there is no header enrichment, a HTTP 302 redirect is triggered to the Member's hosted server. This step is conducted only for user recognition purposes and therefore it is a 302 backend redirect. The relevant landing page is then rendered, which is via a server under the Member's control, and where the Member applies the required security measures.

11. The Member alleges that the captured logs provided by the complainant demonstrate a HTTP 200 – OK response with all the headers and JavaScript always displayed on the page before the redirect to the network hosted confirmation page.

12. The Member believes that the backend redirect it uses is a more secure way of managing the redirect to the network hosted confirmation page, since the network operator URL is not shared on the relevant JavaScript code and it allows the Member to have more visibility about the users sent to the network operator. This allows the Member to add additional prevention measures through its Fraudwall anti-fraud solution.

Sections of the Code considered

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

14. 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;

15. 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).

16. No further clauses were assigned by WASPA.

Decision

17. 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.

18. 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.

19. 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.

20. 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.

21. 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:

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

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

    21.3 Legacy Browser Exploit Protection.

22. 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.

23. 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.

24. In the present complaint, there is a dispute between the parties as to what the last page was that was rendered immediately before the network hosted confirmation page, and whether or not this page contained the security measures required in section 2.3 of the Guidelines.

25. I have examined the logs provided by the complainant from both tests that were conducted on 16 July 2018 on the Member's system. It is clear from these logs that the last page hosted and/or controlled by the Member immediately before the user is redirected to the network hosted confirmation page did not meet the requirements set out in section 2.3 of the Guidelines.

26. In test number 1, conducted on 16 July 2018 at 14:44, the test result logs (#70256567) show that the last page immediately before the network hosted confirmation page was hosted at the domain – www.pocoyohouse.com (see Header 11 in the logs)

27. In test number 2, conducted on 16 July 2018 at 15:41, the test result logs (#70256550) show that the last page immediately before the network hosted confirmation page was again hosted at the domain – www.pocoyohouse.com (see Header 22 in the logs).

28. In its response, the Member avers that the last page immediately before the network hosted confirmation page is a ''ghost page'' hosted by the Member at the domain – bos.buongiorno.com.

29. The logs do show that there is a redirect to this domain during the subscription flow (see Header 4 for test no.1 and Header 16 for test no.2). However it is clearly evident from the logs provided that this is not the last page before the user is directed to the network hosted confirmation page.

30. The Member has also stated that if there is no header enrichment for user recognition purposes, the relevant landing page is then rendered via the domain – www.pocoyohouse.com, which has all the required security measures in place.

31. The logs do show that this page is rendered and does comply with the requirements set out in section 2.3 of the Guidelines (see Header 5 for test no.1 and Header 17 for test no.2).

32. However this is not the last page before the user is redirected to the network hosted confirmation page. Further redirects then take place for third party hosted services, before the pages at domain www.pocoyohouse.com (shown as ''Header received 11'' and ''Header received 22'').

33. Based on the aforegoing, I am satisfied that the Member has not complied with the best practice requirements prescribed in section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines and, as such, 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.

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

Sanction

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.