Wireless Application Service Providers' Association

Report of the Adjudicator

Complaint number	#39886
Cited WASPA members	Hulk Mobile (1689)
Notifiable WASPA members	Basebone (1344)
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	2018-07-18; 2018-07-28; and 2018-07-29
Applicable version of the Code	v15.5
Clauses of the Code cited	4.11(a)

Related complaints considered	n/a
Fines imposed	Payment of suspended fine of R50 000 for complaint #39136 Payment of R100 000 for contravention of clause 4.11(a) in present complaint
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 three 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 three test results showed that the CSP and X-Frame header requirements had been implemented by the Member, however an ''HTTP 302'' code was provided, which meant that the measures did not render properly and were not effective.

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

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

Member’s response

5. The WASPA member cited as the respondent in this complaint is an affiliate member of WASPA. I will refer to them as the ‘’Respondent’’.

6. The Respondent did not respond directly to the complaint. Instead, another member, who provides services to the Respondent, submitted a response to the complaint on the Respondent’s behalf.

7. For ease of reference, I will refer to the member who submitted the response to the complaint as ‘’the Service Provider’’.

8. The Service Provider alleged in its response that the last page on the domain used by the Respondent, and which is immediately before the network confirmation page, was an *“invisible page tracking clicks/statistics on the Call-To-Action before forwarding to the relevant network hosted confirmation page’’*.

9. The Service Provider also alleged that this ‘’invisible page’’ could not be reached from the outside and only from the preceding page, which was the landing page.

10. The Service Provider alleged that the landing page contained the relevant anti-fraud headers and scripts, and was correctly rendered (i.e. the *‘’HTTP 200‘’* code is displayed).

11. The Service Provider argued that although the measures implemented by the Respondent did not match the requirements of section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines, to the letter, the Respondent had complied, in substance, with the requirements of clause 4.11(a) of the WASPA Code and the end result was that the Respondent’s system was effectively secured.

12. The Service Provider used the following analogy to clarify its position - *‘’the outer door has locks and is closed shut. The inner door is open but cannot be reached from the outside’’.*

13. The Service Provider argued further that although the requirement of having a page on the domain used immediately before the network confirmation page, with all the required

security measures in place, is an imperative for a single-step flow (i.e. where the aggregator simply forwards a request); it was not an imperative in a multi-step flow, where the landing page is rendered first and then after the Call-to-Action is clicked, the forwarding to the network confirmation page takes place from a page that is not vulnerable to attack from the outside.

14. The Service Provider argues that if the Respondent is held in breach of clause 4.11(a) of the Code, and is fined, because of its failure to abide by a literal interpretation of the technical requirements set out in section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines, this could be seen as abusive and against the spirit of the WASPA membership.

15. The Service Provider also confirmed that the Respondent had since modified its technical solution to ensure that the final page rendered before the network confirmation page contains the relevant policies and headers and returns the required HTTP 200 message. However, it added that this technical change is less efficient and prevents some customers from completing their intended purchase.

Sections of the Code considered

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

17. 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;

18. 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).

19. No further clauses were assigned by WASPA.

Decision

20. 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.

21. 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.

22. 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.

23. These best practice measures were published in the Fraud Detection and Mitigation Best Practice Guidelines, version 2.1 of which has been accepted by and is currently binding on all WASPA members.

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

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

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

24.3 Legacy Browser Exploit Protection.

25. 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.

26. More importantly in the context of the present complaint, section 2.3 also expressly stipulates that the prescribed measures must be implemented on the last rendered page on the relevant domain used by the member immediately before the network confirmation page.

27. The pertinent question to be answered in the present complaint is whether the last page rendered on the domain used by the Respondent immediately before the network confirmation page was visible to users and formed part of the subscription flow?

28. If it was, then the prescribed requirements set out in section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines must be implemented for that page.

29. However if this page was not visible to users and was merely used by the Respondent for internal tracking or statistical purposes, as alleged by the Service Provider, then the landing page would be the last page visible to users in the subscription flow.

30. I have reviewed the test results provided by the complainant and it is evident from the relevant logs generated from each of the three tests conducted by the complainant that the last rendered page hosted and managed by the Respondent before the network confirmation page is the page found at the domain: http://snow.fantasticflex.com.

31. I have tested this page and it is readily accessible by clicking on the given URL (tested on 19/9/18 at 7:59am).

32. The logs do show that another page immediately precedes the network confirmation page (i.e. found at http://wap.baseboneconnects.com), which is not accessible externally and appears to merely be used for tracking and/or internal statistical purposes, as alleged by the Service Provider.

33. However this page is not a rendered page and should not be taken into account when adjudging whether the Respondent has complied with the prescribed requirements of section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines.

34. The logs provided by the complainant show that the last rendered page hosted and managed by the Respondent before the network confirmation page (and found at http://snow.fantasticflex.com) did have the required CSP and X-Frame header implemented.

35. However this page returned an ''HTTP 302'' code, which means that these other measures did not render properly and were therefore not effective.

36. The Respondent has therefore failed and/or omitted to comply with the best practice requirements prescribed in section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines.

37. Based on the aforegoing, I am satisfied that the Respondent has contravened clause 4.11(a) of the WASPA Code of Conduct, and the complaint is accordingly upheld.

Sanction

38. 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.

39. 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.

40. The failure of a member to comply with the prescribed measures 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.

41. I have also taken into account, as a further aggravating factor, that the Respondent had a complaint previously upheld against it for the same contravention (see complaint #39136).

42. The Respondent did not provide any mitigating factors to be considered.

43. Based on the aforegoing, the following sanctions are imposed:

43.1 The Respondent must now pay the suspended fine of R50 000 which was imposed by the Adjudicator for complaint #39136 since the Respondent has now been found to have contravened clause 4.11(a) of the Code again within a period of 365 days from the date that the ruling was made for that complaint, i.e. 26 July 2018.

43.2 The Respondent is fined an amount of R100 000.00 for the contravention of clause 4.11(a) for the present complaint.