Wireless Application Service Providers' Association

Report of the Adjudicator

Complaint number	#39139
Cited WASPA members	Marvel Media Sdn Bhd (1514)
Notifiable WASPA members	Netsmart (Incorporated in Republic of Cyprus) (1436)
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	2018-05-18
Date of alleged breach	Same as above
Applicable version of the Code	v15.5
Clauses of the Code cited	14.11(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 a test was conducted on the Member's system and it was identified that the Member had failed 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 complainant alleges that the Member's systems were therefore vulnerable and were not sufficiently secured to prevent potential fraudulent attacks or activity.

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

Member's response

1. The remember initially responded that they were currently working with Netsmart to review and sort out the problem on 21 May 2018. It indicated that certain of the steps have been implemented, but asked further info on "302 Redirect".

2. On 23 May 2018 it sent a second substantive response indicating that they had updated the fraud detection and mitigation steps after coordinating with Netsmart and requested WASPA to retest their landing page.

Sections of the Code considered

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

4. 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;

5. 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.

6. No further clauses were assigned by WASPA.

Decision

7. 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.

8. 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 to take reasonable steps to prevent their networks and systems from being used in a fraudulent manner.

9. These measures include:

9.1 complying with WASPA's published best practices for fraud prevention;

9.2 timeously blocking interactions with specific applications or sources as soon as reasonably possible; and

9.3 timeously reporting any fraudulent activity identified on their networks or systems to WASPA.

10. Following due consultation with its members in the course of a number of workshops, WASPA introduced its Fraud Detection and Mitigation Best Practice Guidelines (the *''Fraud Guidelines''*).

11. Section 2.3 of the Fraud Guidelines sets out certain standards and measures to be implemented by members to prevent or mitigate against user interface redress attacks (including ''clickjacking'' and SOP bypassing).

12. The Fraud Guidelines stipulate that three different measures are to be adopted by members, namely:

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

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

12.3 Legacy Browser Exploit Protection.

13. The Fraud Guidelines expressly state that all three of these measures must be implemented together. If they are not implemented together, the member's system will still be vulnerable to attack.

14. The Fraud Guidelines also expressly state that these measures must be implemented for the page on the relevant domain used immediately before the relevant network confirmation page.

15. In this complaint, the test conducted by the Compliance Department identified that the Member had not implemented the required measures set out in section 2.3 of the Fraud Guidelines.

16. In particular, the test results showed that the page immediately before the network confirmation did not reflect the required CSP and X-Frame-Options headers. The X-Frame-Options show “SAMEORIGIN” instead of ‘DENY”.

17. In its response the Member did not deny non-compliance with the fraud prevention measures as required in terms of the Code of Conduct. Instead, it simply indicated that the problem was addressed immediately in conjunction with Netsmart.

18. Based on the aforegoing, I am satisfied that the Member did not comply with WASPA's published best practices for fraud prevention and has contravened clause 4.11(a) of the WASPA Code.

19. The complaint is accordingly upheld.

Sanction

20. Effective fraud prevention and mitigation is clearly in the best interests of all stakeholders in the industry. Clickjacking poses 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.

21. Furthermore, the measures required to be taken in terms of the published best practice guidelines are relatively easy to script and inexpensive to implement.

22. 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 threat that fraud poses to the industry as a whole.

22.1 The Member did not, in their response to the complaint, provide any mitigating factors to be considered. However, 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 there have also not been any other complaints lodged against the Member.

23. Based on the aforegoing, the member is fined an amount of R100 000, of which R50 000 is payable immediately and a further 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.