Wireless Application Service Providers' Association

Report of the Appeals Panel

Complaint number	39144
Cited WASPA members	Jimstu Telecoms CC (1286)
Notifiable WASPA members	N/A
Appeal lodged by	Jimstu Telecoms CC (1286)
Type of appeal	Panel
Scope of appeal	Review of the decision and sanctions imposed by the adjudicator.
Applicable version of the Code	15.5
Sections considered by the panel	4.11(a)
Related complaints considered	39135, 39138, 39139, 39141 and 39142
Amended sanctions	R100 000.00 fine for a contravention of 4.11 (a) payable on publication of this report, R75 000.00 of such fine to be suspended for 6 (six) months provided 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.
Appeal fee	50% (fifty percent) refund.
Is this report notable?	No
Summary of notability	No

Initial complaint

This complaint related to a failure of the Member 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) and accordingly comply with the requirements of clause 4.11(a) of the WASPA Code of Conduct.

The Formal 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).

Adjudicator's findings

The Adjudicator found as follows:

1. 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.
2. 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.
3. These measures include:
    a. complying with WASPA's published best practices for fraud prevention;
    b. timeously blocking interactions with specific applications or sources as soon as reasonably possible; and
    c. timeously reporting any fraudulent activity identified on their networks or systems to WASPA.
4. 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).
5. The Fraud Guidelines stipulate that three different measures are to be adopted by members, namely:
    a. the Content Security Policy (CSP) standard created by the Worldwide Web Consortium;
    b. the X-Frame-Options Response Header directive; and
    c. Legacy Browser Exploit Protection.
6. 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 and that these were expressly stated as having to be present on the page of the relevant domain immediately before the relevant network confirmation page.

7. 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.
8. 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.
9. In sanctioning the Member, the Adjudicator considered the following:
    a. 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.
    b. The measures required to be taken in terms of the published best practice guidelines are relatively easy to script and inexpensive to implement.
    c. 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.
    d. The Member did not, in their response to the complaint, provide any mitigating factors to be considered.
    e. This is the Member's first offence with regard to a breach of clause 4.11 and there have also not been any other complaints lodged against the Member.
10. The Adjudicator fined the Member an amount of R100 000.00, of which R50 000.00 was payable immediately and a further R50 000.00 was suspended for 6 (six) months. 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.

Appeal submissions

The Member appealed the decision and severity of the Adjudicator's sanctions.

The Member requested that both the decision and the sanctions be looked at again in the light of the following circumstances:

1. The Member had interpreted and implemented their interpretation of the Code in good faith;
2. The Code should be interpreted in the spirit of the law and not just the letter of the law;
3. The Member did not admit non-compliance;
4. The breach was an honest difference in interpretation and not merely wilful disobedience;
5. The Complainant suffered no loss;

6. The Member had no consumer complaints relating to this;
7. The Member has not had any complaints against it before;
8. The Member felt with all of their other fraud mitigation practices in place, even without compliance with the Code their solution offered more protection than WASPA's requirements.

In respect of the severity of sanctions for the breach of 4.11(a) the Member viewed these as unduly harsh.

The Member accordingly requested that the decision and sanctions be amended.

Deliberations and findings

The panel reviewed the complaint files, the Adjudicator's report as well as the Member's appeal.

The Code of Conduct mandates that an Adjudicator must do as follows when sanctioning a Member (our highlights):

"24.33. On the basis of the evidence presented, the adjudicator will decide whether there has been a breach of the clauses of the Code identified in the complaint. Each case will be considered and decided on its own merits. **When making adjudications and determining sanctions, previous precedent should be taken into account. Precedent set by appeals panels should carry more weight than that set by adjudicators.**

"24.34. If the adjudicator determines that there has been a breach of the Code, then the adjudicator must determine appropriate sanctions. **In determining any appropriate sanctions, the adjudicator must take into consideration:**
(a) any previous successful complaints made against the respondent in the past three years;
(b) any previous successful complaints of a similar nature;
(c) the nature and severity of the breach;
(d) the loss suffered by the complainant;
(e) any efforts made by the respondent to resolve the matter; and
(f) any other factors that the adjudicator considers material."

In sanctioning the Member, the Adjudicator considered the following:

1. 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.
2. The measures required to be taken in terms of the published best practice guidelines are relatively easy to script and inexpensive to implement.

3. 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.
4. The Member did not, in their response to the complaint, provide any mitigating factors to be considered.
5. This is the Member's first offence with regard to a breach of clause 4.11 and there have also not been any other complaints lodged against the Member.

In addition, the Adjudicator's sanctions are in line with current precedent for breaches of the same nature, and in fact are on the lower end of the scale.

The Member raised the issue of the spirit versus the letter of the law several times in their argument. Whilst certainly the spirit of the law is looked at for guidance in the event of an ambiguity or lack of clarity, it doesn't offer an opt out from compliance in the event where there is no ambiguity. The member failed to implement the necessary fraud protection measures as required by the Code on the page of the relevant domain immediately before the network confirmation page. This requirement is not ambiguous or requiring interpretation. The measures are either there or they are not. In this case they were not. In addition, it is not up to the Member to determine how to interpret and apply the requirements of the Code of Conduct where they are very clearly stated. Should the Member disagree with what is set out in the Code they must continue to comply with the Code but should take this up with the Code of Conduct committee with a view to putting forward their proposal to see if the Code can be amended.

The Member also raised the fact that they had not admitted to not complying with the Code. If the Code of Conduct could only be enforced if the Member admitted non-compliance it would render the Code toothless and the adjudication process farcical.

The panel is of the view that although the Member responded pro-actively to remedy the breach and mitigate the risks, and although the Member had implemented their own fraud mitigation practices, they still breached the Code, and this was still a serious breach of the Code. However, they have demonstrated the fact that they take the issue of fraud seriously in their choice to implement additional fraud prevention technical measures and have behaved with good faith in their willingness to abide by the Code of Conduct. Accordingly, although the panel agrees with the adjudicator's decision, we have decided to amend the sanctions to reflect the particular scenario of this case.

Amendment of decision and sanctions

For the reasons set out above, the decision is not amended. The sanctions are amended R100 000.00 fine for a contravention of 4.11 (a) payable on publication of this report,

R75 000.00 of such fine to be suspended for 6 (six) months provided the 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.

Appeal fee

The Member has been partly successful in the Appeal and the panel orders a refund of 50% (fifty percent) of the Appeal fee.
