Wireless Application Service Providers' Association

Report of the Adjudicator

Complaint number	#39141
Cited WASPA members	DATA SMS SOUTH AFRICA (PTY) LTD (0151)
Notifiable WASPA members	NONE
Source of the complaint	WASPA Compliance Department.
Complaint short description	Non Implementation of fraud prevention measures
Date complaint lodged	18 May 2018
Date of alleged breach	Unknown

Applicable version of the Code	15. 5
Clauses of the Code cited	4.11 (a)
Related complaints considered	None.
Fines imposed	R 100 000,00 (One hundred thousand rand) payable and R 50 000,00 (Fifty thousand rand) Suspended for six months from date of publication of adjudication: R 150 000,00 for breach of clause 4.11 (a)
Other sanctions	None.
Is this report notable?	Notable
Summary of notability	*Compliance with the Fraud detection and mitigation document in accordance with WASPA code of good practice should be pivotal to all in the industry as non-compliance would mean detrimental consequence to all. Regular fraud parameters must be set up and tested by WASPs.*

Initial complaint

WASPA conducted a test on WEBCELL – HOTPRIME & SPICY GIRLS and identified that you have failed/omitted to implement the requirements as set out in Section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines.

Your systems are therefore vulnerable and have not been sufficiently secured to prevent potential fraudulent attacks or activity.

• Content Security Policy Directive

• X-Frame Options Response Headers

• 302 Redirect

As such, you are potentially in breach of Clause 4.11(a) of the WASPA Code of Conduct.

We request you to take immediate action to rectify this breach and to align your systems with the procedures as set out in the Fraud Detection and Mitigation Best Practice Guidelines.

Please provide proof of the actions taken in order to comply with the requirements to secure your systems.

Note: **URGENT ATTENTION** is required. Any delay in implementing the required practices may be considered as an aggravating factor for this specific potential breach

---

Member's response

Dear WASPA team

We acknowledge receipt of your notice.

We have contacted the content provider to urge it for immediate action.

Apparently these services have just been launched on a test basis through a new connection with Cell C, and probably the tuning was not as precise as needed.

If we don't hear from them this week we shall suspend the whole campaign.

Kind regards.

Complainant's response

None.

Member's further response

None.

Sections of the Code considered

The following sections of the WASPA Code of Conduct, version 15.5, were considered:

4.11. 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

Decision

I note a failure on the part of the Respondent to adhere to a request provided by the Compliance Department, which reads as follows;

Please provide proof of the actions taken in order to comply with the requirements to secure your systems.

Note: URGENT ATTENTION is required. Any delay in implementing the required practices may be considered as an aggravating factor for this specific potential breach

The reasoning behind the bold, italicized and highlighted portion is to indicate to the Respondent (*and all respondents*) that it is imperative to read the entire complaint and to, at the very least be compliant with their response.

The Respondent failed in that;

1. There was no information provided to the secretariat which would be relevant to the complainant at hand; and

2. This complaint involved potential fraud that was detected by the compliance department testers and there was no proof of any action by the Respondent to comply with the requirements and/ or secure their system.

With that said, I will therefore adjudicate on the facts before me.

Allow me to highlight that I was unable to consider any related complaints as there are none, therefore this concept of fraud via click jacking and / or malware (harmful applications) may just be on the rise as a new phenomenon and the industry as a whole is in danger.

My submissions and findings are based on both the Fraud Detection and Mitigation Policy Document (that *all WASPs were advised of from April 2017 and which has already seen over 13 versions come into existence, with version 2.1 being the latest*) and the WASPA Code of Conduct *"Code"*.

The use of technology in our daily lives has been growing rapidly, more so with persons making use of the web and applications to assist in most tasks.

The complainant has placed on record that:

WASPA conducted a test on WEBCELL – HOTPRIME & SPICY GIRLS and identified that you have failed/omitted to implement the requirements as set out in Section 2.3 of the Fraud Detection and Mitigation Best Practice Guidelines.

Your systems are therefore vulnerable and have not been sufficiently secured to prevent potential fraudulent attacks or activity.

And the response from the Respondent was:

Apparently these services have just been launched on a test basis through a new connection with Cell C, and <u>probably the tuning was not as precise as needed</u>.

I submit that the underlined portion indicates just how flippant WASPs are being when it comes to this new era, further there is not even an indication that there are / was action taken to secure the system.

I find then that it is the end of the chain that is liable and more responsibility must be taken as to ensure that fraud measures are implemented in accordance with clause 4.11(a) read with sub clause 2.3 of version 2.1 of the Fraud detection and mitigation practice best practice document.

The contravention of the clause in its entirety is upheld, I uphold such a breach as one of potential fraud as the Respondent had indicated (*and one shall take it in good faith*) that should they not hear from “them” again, that they will suspend the entire campaign. There was no actual fraud that occurred or a higher sanction would have been imposed.

“Your systems are therefore vulnerable and have not been sufficiently secured to prevent potential fraudulent attacks or activity”

Sanctions

I therefore determine that there was in fact a breach of the code, therefore the cited clause contravention is upheld and I call for the following fine to be imposed on the Respondent, such fine is therefore payable within 7(seven) days of receipt of the adjudication report, and the suspended portion is so suspended for a period of 6 (six) months from date of publication of the report. Should the Respondent breach the cited clause within the six month period, the amount so suspended shall be immediately due and payable.

All fines are directly imposed on Data SMS South Africa (Pty) Ltd (0151).

R 150 000, 00 for breach of clause 4.11(a), R 50 000, 00 of which is to be suspended for a period of six months.

Matters referred back to WASPA

NONE.
