WASPA appeals panel

Complaint 14211

REPORT OF THE APPEALS PANEL

Date: 08 November 2012
Appellant and Information Provider (IP): Opera Interactive / Morvec (IP)
Complaint Number: 14211
Applicable versions: 11

---

1. **BACKGROUND TO THE APPEAL**

1.1 This appeal concerns a complaint initiated elsewhere and followed up by the Monitor in the form of a Heads Up on the 20th of July 2011 with an eventual emergency panel and subsequent formal complaint, lodged on the 12th of August 2011.

1.2 The Appellant and IP are full members of WASPA.

1.3 The complaint related to the issue of “unwanted”, “unauthorised” or “unlawful” subscription.

1.4 In this specific instance the complaint involved a procedure whereby an innocent third party was involuntarily subscribed to a service by another person.

1.5 Although such practice did not initially seem technically feasible, it was subsequently proofed achievable.

1.6 In this particular instance, the SP, IP and WASPA Technical Committee members appeared to have a consensus view that it was technically possible,

even if a double opt in process was employed, for an innocent third party to be involuntarily subscribed to a service by another person.

1.7 The technical responses explained that WASP's are able to receive MSISDN details of a person browsing a WAP site or website even if that person does not manually insert their MSISDN number into the site. This is achieved by the mobile network operator providing the MSISDN details to the service provider by transmitting those details to a designated domain used by the service provider for this purpose.

1.8 However, as the Consumer had highlighted in another complaint (13405), if an innocent party's MSISDN is manually inserted by another person as a variable in the URL query string on the domain used by the relevant service provider to receive MSISDN details from mobile network operators, the innocent party will become involuntarily subscribed to the service.

1.9 The complaints, the findings of the Adjudicator, the SP and IP's response to and appeal against the complaint, are fully recorded in the case files provided to this appeals panel, and as these are, or will be, publicly available on the WASPA website, they will not be repeated in full in this appeal panel's report.

2. CLAUSES OF THE CODE CONSIDERED

2.1 The Appeal relates to alleged breaches of section 3.6.1 of the Code, which reads:

> *Members will take all reasonable measures to prevent unauthorised or unlawful access to, interception of, or interference with any data.*

3. FINDINGS AND DECISIONS OF THE ADJUDICATOR

3.1 Finding of the Adjudicator

In the findings which are relevant to this appeal, the Adjudicator inter alia stated:

Having reviewed the Code, there is no specific provision relating to the degree of security that ought to be applied to subscription processes themselves. Rather, there is a general data protection requirement in section 3.6.1 that *"members will take all reasonable measures to prevent unauthorised or unlawful access to, interception of, or interference with any data"*. A consumer's MSISDN number would, in my opinion, fall within the meaning of the word "data" in section 3.6.1. I do not find that any data was unlawfully "intercepted" in this complaint; however it is clear that the consumer's MSISDN number was accessed and processed without authority.

The crisp question that therefore falls to be considered is whether the SP and IP took *"reasonable measures to prevent"* their unauthorised access to the consumer's MSISDN as required by section 3.6.1.

In this regard, I have had cause to consider the content of complaint number 13405, where the same security vulnerability was first brought to the members' attention by the Consumer. In that matter, the Consumer had provided WASPA with details of the security flaw on or about 2 July 11.

By 5 July 2011 the IP had written to WASPA and stated that it was clear that Consumer had *"created a false MO"* and had *"fraudulently subscrib[ed] another mobile user to a service without their knowledge or consent".*

The Consumer has also previously blogged about the issue and thereby increased the likelihood of the same vulnerability being exploited by others. The SP also wrote to WASPA in complaint 13405 on 5 July 2011 and stated that *"[i]n light of the new evidence and submissions, we have temporarily suspended the services of Morvec Limited on the 4th July 2011 in order to do a full investigation and to ensure that there can be no potential future harm to any affected subscribers. The suspension is done as a preventative measure and a precaution and does by no means constitute an admission of any kind."*

Notwithstanding the undertaking to suspend the service, the present complaint arose on 19 July 2011, some two weeks after the undertaking that the service would be suspended. On 20 July, the IP again advised WASPA that the service would be suspended and also advised that it was in the process of being issued with new "White Label" URLs that it felt would put an end to the hacking.

Although the vulnerability apparently presents itself equally to all service providers offering a similar service, the vulnerability was specifically brought to the attention of the IP and SP at the beginning of July 2011.

The facts of complaint 13405 and the present complaint demonstrate:

i. that the IP and SP knew about the security breach and vulnerability from around 2 July or 5 July 2011;
ii. that the IP undertook to suspend the service on 5 July in order to do a full investigation and to ensure no further harm to consumers;
iii. that on 19 July the service was being operated without the IP having yet properly resolved the vulnerability (the IP stated on 20 July that it would suspend the service and that it was "in the process" of being issued with the white label URLS that it felt would resolve the vulnerability).

On 20 July 2011, the WASPA Monitor asked the SP whether the SP had *"cut off the link to this service"*. On that same day, the SP replied that it had done so and that it was taking pro-active steps to prevent any future harm to consumers.

On 26 July 2011 the Monitor in turn advised the technical committee members of WASPA that the service had been suspended.

On 4 August 2011, the service was re-tested and found to still be active.

In a letter to WASPA dated 11 August 2001, Oxygen8 advised that at length as follows [own emphasis added]:

The Heads Up was received and both the Service Provider and the Information Provider responded. In the various communications with regards to the Heads Up it was indicated that ***due to outside human intervention the normal double opt in process was compromised****.*

[The Consumer] hacked into the normal double opt in process by interfering with the Cell C MSISDN pass-through procedure and subsequently he auto-subscribed certain numbers. He did this on a normal PC. He also posted this method on his personal blog site as well as the MySpace blog site with the result that various people with a bit of an IT background could have followed his example.

The normal process which consisted of a compliant WAP banner that contains the necessary information which if clicked (first opt-in) on directs the person to a WAP Confirmation Page, and in turn if the person clicked on the 'join' or similar button on the WAP Confirmation Page (second double opt-in) would initiate the subscription was compromised. [The Consumer] entered the numbers manually on his PC using the Cell C MSISDN passthrough process, which step normally would form part of the second opt-in step, and thus by-passing the first opt-in step.

On receipt of the Heads Up the Information Provider change the access URL's of the service as a preventative step. However, the fault in the procedure was not due to a lack in security settings of the Information Providers Service, but due to the process used by Cell C to do MSISDN pass-through. This fact was confirmed in the response from WASPA when WASPA confirmed that the Heads Up was closed.

The test done by the Media Monitor post the closing of the Heads Up was flawed. The tester used the URL link in the MySpace blog which all parties concerned are aware is compromised, as it is the link provided by [the Consumer] to prove that a person can manually auto-subscribe any number. This URL link bypasses the first opt-in request and subsequently is obvious that there will not be a double opt-in present. This links initiates the process at the WAP Confirmation Page as entry point. ***The compromised link is by no means a representation of the service as it functions normally.***

…

The service is currently live, new subscribers can join and billings for the service are active. In light of the fact that our report will show that the service is functioning effectively and that the Heads Up was based on an surreal outside human intervention occurrence, which was confirmed by WASPA; and that the test done post the Heads Up was done by utilizing the already proven compromised link, which renders such test flawed and not accurate; there is no reason for the service not to be live.

I regard the failure of the IP and SP to suspend the services indefinitely from 5 July 2011 until such time as reasonable measures had actually been taken to properly address the vulnerability as a failure to *"take all reasonable measures to prevent"* unauthorised access to the consumer's MSISDN for subscription purposes as required by section 3.6.1 of the Code. The IP was fully aware of the vulnerability and was quick to characterise the Consumer as a criminal and was aware that he was publishing details of the exploit online. In such circumstances, the IP and SP ought to have acted with far greater caution. If they had, this second complaint might not have arisen on 19 July 2011. The IP could, ostensibly, have waited until the white label URLs had actually been issued before reactivating the service or it could have simply revised its WAP subscription processes temporarily to require SMS based confirmation of new subscriptions.

The SP and IP have accordingly breached section 3.6.1 of the Code.

3.2 Sanctions

For the breach of section 3.6.1 of the Code, fines of R10 000 are imposed on each of the IP and SP respectively.

Section 14.5.1 of the Code provides that where an adjudicator has reason to form an opinion that an information provider may persist in operating a service in breach of any section of the Code, the adjudicator may instruct the Secretariat to issue a notice to WASPA's members. In light of the obvious security vulnerability exposed by the Consumer and the failure of the SP and IP to fully suspend the service indefinitely pending adequate resolution of the vulnerability, I am of the opinion that an information provider notice is justified in this matter. All members should kindly be

made aware by formal notice from the Secretariat that any member who permits the information provider to operate a service in a manner that exposes any third party to involuntary subscription in the specific manner highlighted in the present complaint may, after a period of 5 business days from the date of publication of the notice, be deemed to be in breach of section 3.6.1 of the Code and may be subject to sanctions should complaints of a similar nature be upheld against them.

4. GROUNDS OF APPEAL

Grounds of appeal for complaint 14211:

4.1 The Appellant is appealing the decision relating to the Adjudicator's interpretation and use of section 3.6.1.

4.2 The Appellant submitted various instances for its grounds, inter alia:

4.2.1 Suspension of services;
4.2.2 Technical/security flaw in the MSISDN forwarding process of CELLC; and
4.2.3 Steps taken to address the technical /security flaw.

5. FINDINGS OF APPEAL PANEL

5.1 Version of the Code

5.1.1 The complaint was made over a period correlating with version 11 of the Code. Version 11.0 of the Code applied from 8 June 2011 to 17 November 2011 and is therefore the correct version for this matter.

5.2 Finding

5.2.1 Right from the outset this Panel has to confess that the issue in front of it is not the substance of a clear cut scenario.

5.2.2 The Panel has therefore duly analysed the Adjudicator's specific reasoning behind his or her decision reached on the basis of section 3.6.1 and weighed the reasonability of the subsequent findings and sanctions related thereto.

5.2.3 The Panel has also duly analysed the response offered by the Appellant in its Appeal and in particular paid attention to the difficult position the Appellant finds itself with regards to the alleged and subsequently proofed operating flaw, which from a security perspective, might infer the Appellant's breach of section 3.6.1 of the WASPA Code.

5.2.4 The Panel found it therefore only appropriate to once again rephrase section 3.6.1 of the Code that was made the subject clause of the alleged breach by the Appellant.

5.2.5 Section 3.6.1 states that: *Members will take all reasonable measures to prevent unauthorised or unlawful access to, interception of, or interference with any data.*

5.2.6 The first question that should be uttered: Do *all reasonable measures* to be taken by Members *include* matters beyond their control?

5.2.7 Although the initial answer might seem to be in the negative, this Panel is of the opinion that where such an action / s (all reasonable measures) by the Member could prevent the happening of a matter / event beyond the Member's control, then the *subjective* answer could, although abstrusely, still be debated in the affirmative.

5.2.8 However of even greater importance to this Panel is to underscore what is regarded or meant as *reasonable*?

5.2.9 Various factors influence whether a particular measure is considered reasonable. The test of what is reasonable is ultimately an *objective* test and

not simply a matter of what one may personally (subjectively) think is reasonable.

5.2.10 When deciding whether a measure taken is reasonable one can consider:

5.2.10.1 how effective the change by a Member or the Appellant in this matter will be in avoiding the disadvantage the potential subscriber / customer would otherwise experience;

5.2.10.2 the measure's practicality

5.2.10.3 the cost to the Member and Appellant in this matter

5.2.10.4 the Member's resources and size.

5.2.11 In light of the above the Panel does not feel that the continued suspension of one individual SP and / or IP's services could practically benefit the industry as a whole or public at large and this Panel is therefore of the opinion that the security flaw is beyond the Appellant's control and therefore outside the ambit of what is considered a reasonable measure in terms of cost or loss of income for the Appellant weighed up against the potential damage of a potential customer or innocent third party, caused by a factor (Cell C flaw) beyond its own control..

5.2.12 The Cell C security flaw is further exacerbated by the fact that it was maliciously and unlawfully exploited by an outsider (possible hacker) and not conducted in the normal course of day to day operations.

5.2.13 What might be considered as reasonable security measures is also difficult to ascertain, as clearly illustrated by this little insert of FBI director Robert Mueller when ~~quoted in a CNN Money story~~ on the data security crisis now facing American businesses – an issue of particular importance to small businesses:

There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again.

5.2.14 The fact that the Appellant has brought the technical/security flaw in the MSISDN forwarding process of Cell C to the attention of WASPA and the mere fact that the Appellant, upon receipt of the Report of the Adjudicator requested the assistance of the WASPA Management Committee to investigate the matter and assist in liaising with the Mobile Network Operator Cell C in order to find a solution to the problem, reveals to this Panel what is regarded in this matter as all reasonable measures.

5.2.15 **The decision relating to section 3.6.1, and all the relevant sanctions referred to in paragraph 3.2 above is therefore overturned.**

5.2.16 This Panel is however concerned about the obvious security flaw at Cell C and the WASPA Secretariat is advised to take urgent and immediate steps to raise the issue with the WASPA Mancom so that the issue can be addressed as a matter of urgency.

5.2.17 It is also advised that WASPA issues immediate notices to all its members informing them of the current Cell C security flaw, also simultaneously directing its members with any alternative mechanisms whereby interim solutions to the flaw could be found, if possible.

5.2.18 This should be prioritised as an imperative prerogative.

5.2.19 **The cost of appeal is refundable.**