REPORT OF THE ADJUDICATOR

Complaint reference number:	14211
WASPA member(s):	Opera Interactive t/a Oxygen8 (SP) / Morvec (IP)
Membership number(s):	0068 / 1137
Complainant:	Monitor
Type of complaint:	Subscription
Date complaint was lodged:	2011-08-01
Date of the alleged offence:	2011-07-19
Relevant version of the Code:	11
Clauses considered:	3.6.1; 11.2.1; 11.9.4; 14.5.1
Relevant version of the Ad. Rules:	Not applicable
Clauses considered:	Not applicable
Related cases considered:	#13405

Complaint **and Responses**

The present complaint has arisen as the ultimate result of the Monitor receiving a notification from a complainant of involuntary subscription to a service operated by the IP in conjunction with the SP.

The complaint pack forwarded to me for review comprises of some 59 separate emails and supporting documents and I do not propose, nor think it necessary, to summarise the contents of each document in this report.

The following are the salient facts for the purposes of this report:

1. A complainant advised the Monitor that he had been involuntarily subscribed to the “Go Go Mobile” subscription service operated by the IP in conjunction with the SP. Although the complainant took steps to unsubscribe from the service, he appeared to be continuously re-subscribed.

2. The response of the IP was that an aggrieved consumer (who was himself a complainant in complaint number 13405 lodged against the same IP and SP and who is hereafter referred to as “the Consumer”) had engaged in the conduct of involuntarily subscribing third parties to the IP’s service in an apparent attempt to expose what he regarded as unsecure billing practices of the IP and SP. The IP advised that it was aware of the problem and had identified

the Consumer as the real source of the conduct complained of in this particular matter. The IP advised that its logs revealed that the complainant in the present matter had in fact been subscribed from an Internet protocol address that matched an address that had been identified as being used by the disgruntled Consumer. The IP regarded the Consumer as a hacker who was acting unlawfully.

3. The Consumer himself was neither a party nor a respondent to the complaint.

4. The Monitor enquired how it was possible for the Consumer to actually subscribe third parties to a subscription service if a double-opt in process was in place for the service.

5. Responses to the queries raised by the Monitor were received from the SP, the IP and two representatives of the WASPA Technical Committee.

6. The SP, IP and 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.

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.

8. However, as the Consumer had highlighted in 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.

9. The Technical Committee members agreed that the above vulnerability was not unique to the SP and IP but would be present for any service provider offering a similar service.

In addition to the security issue described above, other issues were raised by the Monitor during the course of the complaint, namely that pricing for the relevant service was advertised using "ZAR" to denote currency rather than "R" and that further testing of the service carried out by WASPA had demonstrated that the keywords "CANCEL" and "END" did not operate to unsubscribe a user. These observations were not disputed by the IP and the issues were rectified.

Decision

This case highlights a significant security flaw in the technical systems and processes used to activate subscription services. The issue undoubtedly requires the urgent attention of both WASPA and the networks.

The question that falls to be determined in this report is whether any breach of the Code has occurred.

Section 11.2.1 of the Code provides that *"customers may not automatically be subscribed to a subscription service without specifically opting in to that service"*.

That a consumer has been subscribed to a service without specifically opting in to the service is clear. The Code however prohibits this from being done "*automatically*".

In my opinion, "*automatically*" implies of the opposite of "*manually*" and the technical security flaw exposed in this complaint and by which the consumer was subscribed to the service resulted from a deliberate, manual insertion of the consumer's MSISDN into a URL query string. Although this was not done by the consumer himself, the involuntary subscription was not "*automatic*" within the meaning contemplated by section 11.2.1 and the SP and IP are not guilty of having *"automatically"* subscribed a consumer to a subscription service.

Section 11.2.1 of the Code was therefore not breached.

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 pass-through 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.

In addition, and by its own admission, the IP breached section 6.2.8 of the Code through its failure to use the required format for pricing information as well as section 11.9.4 through its failure to honour all stop requests using the keywords expressly listed in section 11.9.4.

Sanctions

The breaches of 6.2.8 and 11.9.4 were not raised by the complainant but were revealed by the Monitor on investigation of the service. The SP took steps to remedy these deficiencies.

In the circumstances I impose a minor fine of R1 000 on the IP for breach of section 6.2.8 and a fine of R5 000 on the IP for breach of section 11.9.4.

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.