WASPA
WIRELESS APPLICATION SERVICE PROVIDERS' ASSOCIATION

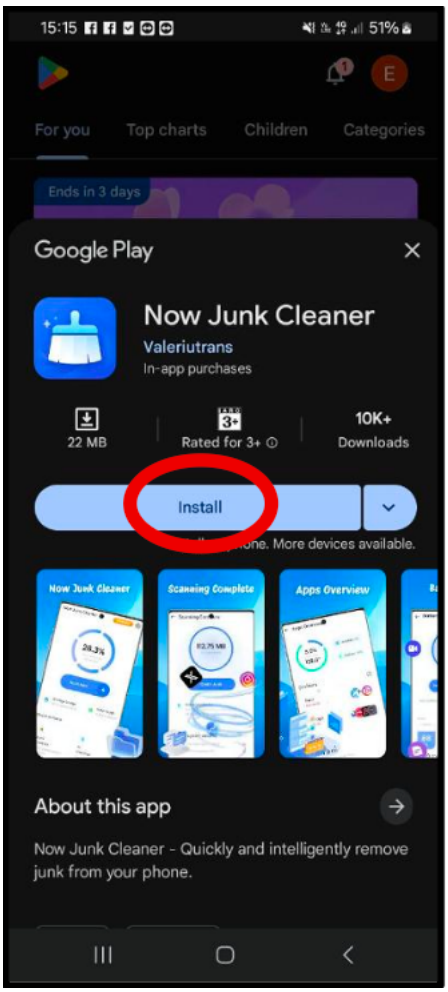
Report of the Adjudicator

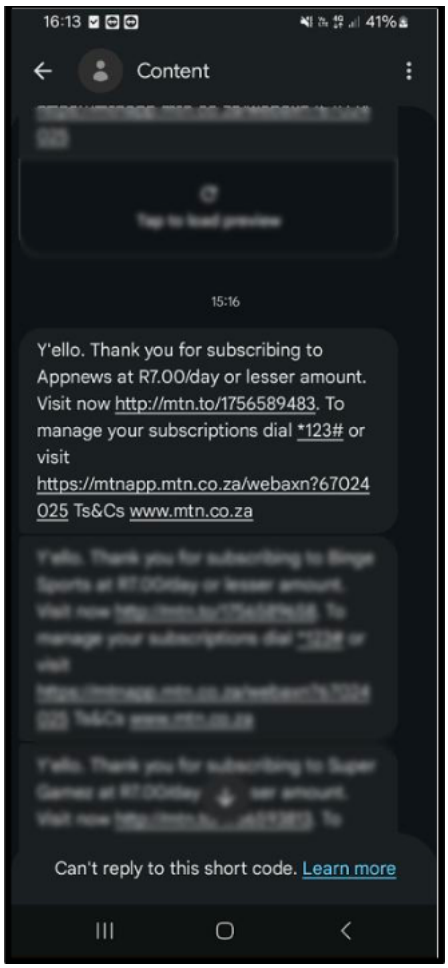
Complaint number	#62094
Cited WASPA members	Worldplay Membership no: 0015
Notifiable WASPA members	n/a
Source of the complaint	WASPA Compliance Department
Complaint short description	Auto-subscription of subscription services
Date complaint lodged	*17 March 2026*
Date of alleged breach	17 March 2026
Applicable version of the Code	*17.14*
Clauses of the Code cited	*4.2; 4.11; 5.4; 5.5; 12.1 read with 8.9; 15.8B; 15.9; 15.10; 23A.5*
Related complaints considered	n/a
Fines imposed	R2 000 for the breach of clause 4.11.
Other sanctions	• All current subscribers to the "Appnews" subscription service must be unsubscribed. • The "Appnews" service itself as provided by the Member must be terminated.

	• The Member must reimburse all subscription fees paid by customers for the “Appnews” service to the extent that they are able to identify such customers.
Is this report notable?	Yes
Summary of notability	• Member not liable for breach of WASPA Code of Conduct if breach due to actions of a malicious third party • WASPA Fraud Detection and Prevention advisory should be updated.

Initial complaint

1. The WASPA Compliance Department (the “Complainant”) provided a formal complaint of an event on the 17th March 2026 on the MTN network where the Member’s subscription service called “App News” was activated on the tester’s cell phone.
2. After the installation of the “Now Junk Cleaner” application (see screenshot below) the tester received a Welcome Message informing the tester that they had been subscribed to a subscription service called “Appnews” at R7.00 per day.





3. The tester did not:
   3.1. Receive any pricing information,
   3.2. Receive or see any promotional material,
   3.3. See any landing page,
   3.4. See any Network (MTN) hosted confirmation page,
   3.5. Have an opportunity to consent.
4. In short, the tester was auto-subscribed to the Appnews subscription service with none of the required steps preceding a subscription service as required by the WASPA Code of Conduct.
5. As a result of this report, the WASPA Secretariat then initiated Emergency Procedure due to the high likelihood of immanent harm to the public.

Member's response

6. The Member then responded on the same day as the complaint was lodged stating:
   6.1. The service had already been identified by their fraud prevention partner and was immediately stopped,
   6.2. The Member then indicated that they were an aggregator and asked if their partner – "Mobichart / Trendy Hot Stuff" was still a WASPA member so that the complaint can either be directed to them or "appropriate action" would be taken by the Member for what amounted to a breach of their agreement with the partner?
   6.3. The Member "fully acknowledge the seriousness of the breach and had already taken steps to contain it."
   6.4. The Member also indicated it will follow up on why the MTN fraud prevention service did not discover the fraud.
7. The Member then also provided another communication on the 19th March 2026 where it indicated:
   7.1. On the 16th March 2026 the Member's fraud prevention partner – MCP – identified the "Appnews" service as potentially fraudulent. It was discovered that this auto-subscription was not part of the service but rather a result of Malware present within the application and was not blocked by the MTN secure-D layer. The Member then blocked the service, stopped acquisitions and started a review of the scope and impact and provided a screenshot of subscribers (862 subscribers as of the 16th March 2026).
   7.2. On the 17th March 2026 MTN then raised the service with the Member, followed shortly by the WASPA complaint. The Member then deactivated the service completely, unsubscribed the entire subscriber base and started a refund of subscribers.
   7.3. The Member then also discovered that the partner Mobichart / Trendy Hot Stuff was not a WASPA member which led to the termination of the Member's relationship with this partner, and proof of this letter (dated 18th March 2026) was provided on the 19th March 2026 by the Member. As part of this communication the Member states: "*In addition, it has come to our attention that you are no longer an active WASPA member, as per our agreement, valid WASPA membership is a strict requirement, and services should not be live in South Africa without a valid and compliant membership in place.*"
   7.4. In terms of impact the Member provided a screenshot of the revenue share and alleged the following:
      7.4.1. Total subscribers: 825

7.4.2. Total revenue over 4 months: R10 888

7.4.3. Partner share: approximately R5000

7.5. The Member further indicated that, in its opinion, this was a “unique malware-related incident that occurred over a short period”.

7.6. The Member then concluded that it proactively identified the error, took steps before being informed by WASPA / MTN, stopped the service, unsubscribed the subscribers and started refunds to subscribers. The malware-related nature of the incident was unusual and the Member took steps to protect its platform and the wider WASP industry.

WASPA Compliance Department response

8. The WASPA Compliance Department responded on the to the Member’s submissions on the 30th March 2026 and argued that the Member did not have sufficient preventative or compliance mechanisms in place without providing any indication of what the Member should have done to prevent the incident and stressed that the actions by the Member should not result in the Member being absolved of liability. The Complainant continues that stopping services and terminating partner relationships after the fact “does not mitigate liability for breaches observed at the time of testing”.

Member’s response

9. In the final submission on the 7th April 2026, the Member indicated that:

9.1. The actual service was not designed in a fraudulent way, but was rather corrupted by malware,

9.2. It had continuous real-time transaction monitoring,

9.3. Integration with MCP fraud detection systems,

9.4. Anomaly detection based on behavioural patterns,

9.5. Immediate suspension and escalation protocols,

9.6. Partner compliance and onboarding controls.

10. The Member continued:

“In this case:

- *The activity was not identified or blocked by upstream network-level protection (MTN Secure-D)*
- *The abnormal behaviour was detected by Worldplay's monitoring systems in real time*
- *The service was suspended within approximately 2 hours of detection*
- *All further acquisitions were immediately prevented from that point forward*

This demonstrates that:

- *Real-time monitoring and detection mechanisms were operational and effective*
- *Immediate containment controls successfully prevented ongoing harm*
- *The system functioned as designed in response to an external threat*

While pre-emptive blocking of all malware-driven activity is not always technically feasible, the Code requires members to take reasonable steps to prevent fraudulent use, which includes the ability to detect, respond to, and contain threats as they arise.

We therefore submit that Worldplay's controls meet and exceed the standard of reasonable preventative measures, when considered in the context of real-world threat environments."

11. The Member further submitted that it had all reasonable compliance systems and argued that the imposition of strict liability was not consistent with the "reasonable steps" as set out in clause 4.11 of the WASPA Code of Conduct.
12. The Member further repeated the steps it had taken to remediate the problem (which have already been detailed above) and confirmed all customers who were subscribed during the 4-month period were issued full refunds and provided proof thereof.
13. The Member further acknowledged responsibility for the service but argued that the breach was neither negligent nor deliberate but was caused by external malware and identified by the Member's own systems.
14. The Member also indicated that the failure of the subscription process (clauses 15.8B, 15.9, 15.10 , 23A.5) were not present in the service as designed by rather inserted there by the malware and so were not a deliberate or negligent decision by the Member or the partner. As a result, it would be unfair to find the Member was in breach of these clauses as neither the Member nor the Partner had designed the subscription process to ignore / avoid these requirements.
15. The Member further submitted that Worldplay has a good record with compliance and took good faith actions before, during and after the incident.

16. The Member then concluded by stating it met its WASPA obligations by taking reasonable steps to prevent, detect and contain fraud.

Adjudicator request

17. After considering the submissions on the 13th April 2026 the Adjudicator sent a communication to the WASPA Secretariat asking it to indicate if the Member was ever informed that Mobichart / Trendy Hot Stuff was no longer a member of WASPA? In addition, if the Member was informed then a copy of the communication should be provided to all parties in order for them to comment thereon.
18. On the 28th April 2026 the WASPA Secretariat indicated that the Member was not informed by WASPA that “Mobichart / Trendy Hot Stuff” was no longer a member of WASPA. The Secretariat further indicated that Mobichart / Trendy Hot Stuff had ceased being a WASPA member on the 01 May 2022.

Second Adjudicator request

19. In addition to the above request, the Adjudicator further requested that the Member provide proof that it had complied with WASPA’s best practices for fraud prevention as referred to in clause 4.11.
20. In response to this request, the Member provided a 4-page document which dealt with the aspects as required by the WASPA fraud prevention and detection and alleged that not only did it comply with the requirements but that the requirements themselves were created approximately 12 years ago and should be updated.
21. As the WASPA fraud detection and prevention document is an internal document in order for the fraud detection and prevention measures not to be publicly known, the feedback by the Member is similarly not included in this adjudication in order to maintain this confidentiality. However, it is worth noting that the Member did demonstrate compliance with the WASPA fraud detection and prevention requirements.

Clauses of the Code considered

3.7. A member is liable for any breaches of this Code of Conduct resulting from services offered or marketed by a client, supplier, affiliate or sub-contractor if that party is not also a member of WASPA. If the member can demonstrate that they have taken reasonable steps to ensure that that party provides and markets services in a manner consistent with the requirements of this Code of Conduct, this must be considered as a mitigating factor when determining the extent of the member's liability for any breaches.

4.2. Members must at all times conduct themselves in a professional manner in their dealings with the public, customers, other service providers and WASPA.

4.11. Members must take reasonable steps to prevent their networks and systems from being used in a fraudulent manner, and must comply with WASPA's published best practices for fraud prevention.

5.4. Members must have honest and fair dealings with their customers.

5.5. Members must not knowingly disseminate information that is false or deceptive, or that is likely to mislead by inaccuracy, ambiguity, exaggeration or omission.

8.9. A "call-to-action" is any link, input box, short-code, or any other component of an advert which triggers the confirmation step for a transaction or a service. In the case where a mobile network operator provides a two-stage confirmation process for the service, the first page of this confirmation process may be considered to be the call-to-action.

12.1. For any web page, pricing information must be displayed for premium-rated services or when a mobile network operator prescribes specific advice of charge requirements. For these services, where there is a call-to-action, pricing information must be clearly and prominently displayed adjacent to the call-to-action.

15.8B. A customer must not be subscribed to any subscription or notification service without completing a confirmation step.

15.9. The confirmation step for any subscription service must require an explicit response from the customer of that service. The confirmation step may not be performed in an automated manner in such a way that the process is hidden from the customer.

15.10. For all subscription services initiated via a web page, there must be an additional specific confirmation step before the customer is billed. This confirmation step must be provided in one of three ways:

(i) The customer's mobile carrier may implement the confirmation step.

(ii) The member can provide the customer with a "confirmation page".

(iii) The member can send a "confirmation message" to the customer. The customer must not be charged for the confirmation message.

Decision

22. This complaint raises a somewhat difficult question which does not appear to have been dealt with before, specifically the liability of a Member for actions that were not taken by it but were rather the result of malware / malicious code.
23. Clause 3.7 of the WASPA Code of Conduct provides that a Member is responsible for the actions of any of its affiliates / sub-contractors. However, this clause does not extend this responsibility to situations where a malicious third party was able to unlawfully access the Member's systems and change them in such a way as to breach the WASPA Code of Conduct. If we are to accept that the Member's systems were affected by Malware and the "service" that was thereafter offered was effectively offered by the hacker - rather than the Member - it cannot be reasonable to find that the Member breached clauses 4.2, 5.4, 5.5, 12.1, 15.8B, 15.9, 15.10 not because the service did not breach those clauses – it clearly did – but because these breaches of the Code of Conduct were not due to the actions by the Member, its affiliates or sub-contractors. Based on the evidence provided to date this is exactly what occurred, and so it is for this simple reason that the complaints regarding clauses 4.2, 5.4, 5.5, 12.1, 15.8B, 15.9, 15.10 are dismissed.
24. This is not, however the end of the matter, as clause 4.11 remains. Clause 4.11 requires that, "Members must take reasonable steps to prevent their networks and systems from being used in a fraudulent manner **and** must comply with WASPA's published best practices

for fraud prevention." (our emphasis)

25. It is worthwhile to separate out the requirements of clause 4.11 into two parts, namely:
    25.1. The Member must take reasonable steps to prevent their networks and systems from being used in a fraudulent manner, and
    25.2. The Member must comply with WASPA's published best practices for fraud prevention.
26. In response to the request for information about the implementation of the WASPA best practices on fraud detection and prevention, the Member provided sufficient evidence to support that it had complied with the requirements of that document. But that still is not the end of the enquiry as this does not deal with the first phrase.
27. Clause 4.11 of the WASPA Code of Conduct requires that the Member take all "reasonable steps" to prevent fraud. These are not steps which are mandated by WASPA, but rather "reasonable steps" which the Member, based on its own security standards, considers to be "reasonable" to prevent fraud. This is the self-same standard that section 17 of the Protection of Personal Information Act (POPIA) mandates that a Responsible Party (i.e. the Member) put into place.
28. By its own admission, the Member indicated that it would not deal with any party who was not itself a member of WASPA. This in turn means that the Member itself considered it to be a "reasonable step" to prevent fraud to ensure that the party was and remained a WASPA member.
29. When this complaint was lodged the Member investigated the status of its affiliate "Mobichart / Trendy Hot Stuff" and, upon discovering that it had ceased to be a Member, summarily terminated their agreement due to the breach of the agreement by Mobichart / Trendy Hot Stuff. However, it transpired that despite "Mobichart / Trendy Hot Stuff" ceasing being a WASPA member on 01 May 2022, the Member remained unaware of this until March 2026. While it may not be reasonable to expect WASPA Members to constantly check the membership status of their partners/affiliates, a relatively frequent check, for example once a quarter, would have alerted Worldplay that Mobichart / Trendy Hot Stuff had ceased being a WASPA member several years ago.
30. It is also worth noting that WASPA normally informs affected Members of the resignation of affiliates, but it failed to do so in the present case.
31. As a result, the only question that remains is whether the Member failed to take a "reasonable step" to prevent fraud by failing to check the WASPA membership status of affiliates for a period of approximately four years? The answer to this must be in the

affirmative and as a result the Member is found to have breached clause 4.11 of the WASPA Code of Conduct.

Sanction

AGGRAVATION

32. The infringement of the WASPA Code of Conduct was extreme and all the sections named by the complainant were in fact breached, just not by the Member. The effect of this on the industry in general is extremely serious – indeed these types of breaches can be an existential threat to the WASP industry.

MITIGATION

33. In many complaints the Member takes insufficient steps to identify the breach of the code of conduct and to provide comprehensive and substantive replies to the WASPA Adjudicator. This is not such a case. The Member took almost all of the reasonable steps to prevent the malware attack and the consequent breach of the WASPA Code of Conduct and then reacted appropriately when the fraud was discovered. The Member is to be commended for its approach to this matter and the actions of the Member not only before the complaint was lodged but also after the complaint was lodged are laudable. Even though the effect of the malware on consumers was substantial, these actions by the Member are very significant mitigating factors which strongly influence the size of the fine imposed.
34. A further set of mitigating factors is that the Member has already unilaterally stopped the service, terminated the contract of the affiliate and initiated a refund of customers.
35. The Member was not informed that Mobichart / Trendy Hot Stuff ceased being a WASPA Member by the WASPA Secretariat.

SANCTION

36. The Member is hereby sanctioned as follows:
    - 36.1. All current subscribers to the “Appnews” subscription service must be unsubscribed.
    - 36.2. The “Appnews” service itself as provided by the Member must be terminated.
    - 36.3. The Member must reimburse all subscription fees paid by customers for the “Appnews” service to the extent that they are able to identify such customers.

(Note: The above is to confirm steps that the Member has already taken)

36.4. The Member is hereby fined the amount of R2000 for the breach of clause 4.11.

Matters referred back to WASPA

37. None.

Appeal

38. In terms of clause 24.37, the Member may appeal a decision of an adjudicator within 10 days of the release of this adjudication.