Important Update Regarding a Third-Party Cybersecurity Incident

We would like to provide an update to our communication dated 26 June 2026 regarding the recent cybersecurity incident involving MIP Holdings, an authorised third-party technology service provider to Legal Expenses Insurance Southern Africa Limited (LEZA).

MIP Holdings identified unauthorised access to a legacy system used for software development and support activities. At this stage of the investigation, we have not identified evidence that LEZA's core operational systems, Member databases, or transactional platforms were subject to unauthorised access. We are also not aware of any fraudulent use of information associated with the incident.

1. What happened?

MIP Holdings identified unauthorised access to one of its legacy development and support systems and immediately activated its incident response procedures. The affected environment has since been secured, and MIP Holdings continues to work with independent cybersecurity and forensic specialists to investigate the incident.

Our investigation is still underway to determine exactly which individuals may have been affected and what specific information may have been involved. Should our investigation determine that Members' personal information was affected, we will contact them directly with details of the specific information involved, the potential implications, and any additional steps they should take.

2. What information may have been involved?

Based on the investigation to date, the categories of information currently being assessed include:

- Personal information, such as names, identity numbers and contact details.
- Membership information.
- Banking details.

At this stage, it has not yet been determined which of these categories relate to individual Members.

3. What are we doing?

LEZA is working closely with MIP Holdings, independent cybersecurity specialists, and legal advisers to understand the full scope and impact of the incident.

LEZA has notified the relevant regulatory authorities, including the Information Regulator, as required, and continues to manage the incident in accordance with the Protection of Personal Information Act (POPIA) and other applicable legal and regulatory requirements.

4. What can you do?

We encourage our Members to remain vigilant, and recommend they:

- Remain vigilant against unsolicited phone calls, emails, SMSs, WhatsApp messages, or social media messages requesting personal or financial information.
- Never disclose passwords, PINs, one-time passwords (OTPs), banking verification codes, or other confidential information.
- Carefully verify the identity of anyone claiming to represent LEZA, their bank, or another organisation before providing any personal or financial information.
- Monitor bank accounts and report any suspicious transactions immediately.
- Monitor their credit profile for any unusual activity.
- As an additional precaution, Members are encouraged to register with the Southern African Fraud Prevention Service (SAFPS) for added protection against identity fraud. Registration is free at **https://www.safps.org.za**.

5. Where can I find more information?

MIP Holdings has published a statement regarding the cybersecurity incident and the actions it has taken in response. You can read the statement here:

https://www.mip.co.za/cybersecurity-incident

Please e-mail popi-informationofficer@leza.co.za should you have any questions or concerns.

Protecting our Members' personal information remains one of our highest priorities. We will continue to provide updates should any new material information become available.