MI-PLAN
Asset Management
Retirement Partners | Analytics

www.miplan.co.za

Tel: 021 657 5960 | Fax: 021 657 5970 | info@miplan.co.za
1st Floor, Mariendahl House, Newlands-On-Main, Newlands 7700
PO Box 23271, Claremont 7735

DATA COMPROMISE - QUESTIONS AND ANSWERS

We are, to say the least, deeply distressed, profoundly shocked and disturbed by this incident. We offer our sincere apologies for the anxiety this incident may have caused. We thank those clients who have shown their support and understanding in these trying times, as well as our staff and service providers who have worked tirelessly to ensure business continuity and the protection of information.

Whilst the initial investigation into and interrogation of the incident has been completed by our cyber-security consultants, the investigation will continue in an attempt to identify the perpetrator of this act of criminality and extortion.

We are committed to protecting our client information and will do whatever our cyber-security consultants advise us is necessary in this regard.

We shall continue to keep you informed should any new information come to light.

We have put together some of the questions we believe you probably have and invite you to communicate directly with us on email info@miplan.co.za or through your broker should you have any specific question we have not addressed.

What is the current status of our IT infrastructure?

There was no breach of the IT system's perimeter, meaning that the IT system remains robust, is and will be able to fully support the business, with no business time or any data lost.

We have been assured by our cyber-security consultants that:

- we have full control of our IT infrastructure; and
- the vulnerability has been addressed and should not happen again; and
- our additional security measures are of an exceptionally high standard.

As an additional precaution, we have initiated our off-site business continuity platform, which has full replicated data, to enable us to seamlessly continue to operate in the event of a full system breakdown, including any further attack.

Are clients' investments affected?

There is no evidence that any client has suffered any financial loss or that their investments have been affected in any way.

MI-PLAN
Asset Management
Retirement Partners | Analytics

www.miplan.co.za

Tel: 021 657 5960 | Fax: 021 657 5970 | info@miplan.co.za
1st Floor, Mariendahl House, Newlands-On-Main, Newlands 7700
PO Box 23271, Claremont 7735

What was the nature of the data compromise?

We need to be circumspect in answering this question so as not to impede our ongoing investigation and that of the authorities. Our cyber-security consultants have advised us that:

- our server access control and identity management complied and continues to comply fully with international best practice; and

- all of our user computers had anti-virus and security software that conformed with international best practice; and

- our security firewalls were not breached before or during the incident; and

- the incident was not as a result of a software exploitation, such as a malware, which would be detectable by machine code, but rather by a highly skilled individual or individuals specifically targeting computers inside a secure network working remotely from home pursuant to the lockdown regulations.

In short, our cyber-security consultants believe that we were the subject of a coordinated social engineering attack specifically targeting our data files for commercial exploitation.

What information has been compromised?

According to the evidence, the perpetrator copied our unstructured files, which comprise Word, Excel and PDF documents, as well as back-up files, which includes at least the following information pertaining to clients, those financial services providers and other service providers or persons doing business with us, as well as past and present staff members:

Individual Client/Entity Details

- the client's/entity's first and last names/registered name; and
- the client's/entity's identity number/registration number; and
- the client's date of birth; and
- the client's/entity's physical address; and
- the client's/entity's email address; and
- the client's/entity's telephone or mobile number; and
- the client's/entity's source of funds and/or wealth; and
- the client's occupation; and
- the client's/entity's investment value thresholds per FICA; and
- the client's/entity's discretionary mandate; and

www.miplan.co.za

Tel: 021 657 5960 | Fax: 021 657 5970 | info@miplan.co.za
1st Floor, Mariendahl House, Newlands-On-Main, Newlands 7700
PO Box 23271, Claremont 7735

- the LISP (Linked Investment Service Provider) contract numbers; and

- the client's/entity's LISP portfolio values; and
- the model portfolio name; and
- the advising FSP/advisor; and

Entity only (where applicable):

- the entity's nature of business; and
- the entity's registration documents; and
- ultimate beneficial owner details (full names, ID number, ownership percentage); and
- authorised persons details (full names, ID number, position); and
- effective person details (full names, ID number).

All identity documents and proof of addresses are encrypted. We have been advised that the encrypted files require decrypting through entering a password or pin code. Our cyber-security consultants advise that there is no evidence that these encrypted files were or have been decrypted.

Financial Advisor Details

- advisor's full name and ID number; and
- FSP name and FSP number; and
- advisor's/FSP's LISP codes; and
- the FSP's physical address; and
- the advisor's/FSP's telephone or mobile number; and
- the FSP's VAT number (if provided); and
- email correspondence with FSP/advisor; and
- the FSP's agreement with MiPlan; and
- the FSP's LISP consultant's name and surname, LISP code, telephone number; and
- investment fund flow reports and product type (where applicable); and

Other data subjects:

- past and present staff records of employment; and

www.miplan.co.za

Tel: 021 657 5960 | Fax: 021 657 5970 | info@miplan.co.za
1st Floor, Mariendahl House, Newlands-On-Main, Newlands 7700
PO Box 23271, Claremont 7735

- FAIS representative and KI records where applicable; and
- company contracts; and
- company contacts and correspondence; and
- manager research and due diligence meetings.

In essence, it is all the information we are obliged to obtain, in law, in the ordinary course of doing business.

What have we done to address the data compromise?

The moment we had reason to believe that there was an incident, we:

- consulted with our IT Infrastructure & Security Provider, iSquared, who are internationally respected cyber-security consultants:
    - who prioritized the immediate protection of our information, which comprises both our business data files and client data files; and
    - whose engineers immediately initiated our off-site business continuity back-up system to have us back online without any disruption should the need arise; and
    - whose forensic team undertook an in-depth investigation and interrogation of our entire IT environment and infrastructure; and
    - whose engineers essentially scrubbed and rebuilt all our machines, as an extra precaution, installing all clean or new software; and
    - who further enhanced our IT infrastructure with security protocols of, we are advised, an exceptionally high standard; and
- notified the Information Regulator in terms of the Protection of Personal Information Act, 2013, as well as the other applicable authorities; and
- started notifying our data subjects, namely those natural and juristic persons affected by the incident, including but not limited to clients, financial services providers and other service providers or persons doing business with us, as well as past and present staff members, in terms of the Protection of Personal Information Act, 2013, by one or more of the following ways, depending on the practicality of the applicable method or circumstances vis-à-vis the client, the financial services provider, service provider or person doing business with us, and our past or present staff member, by email, by placing a data compromise alert and formal section 22(1)(b) notice in a prominent position on our website; by compiling a Question and Answer list on our website and by inviting persons affected to contact us if they have any further queries or something to report.

www.miplan.co.za

Tel: 021 657 5960 | Fax: 021 657 5970 | info@miplan.co.za
1st Floor, Mariendahl House, Newlands-On-Main, Newlands 7700
PO Box 23271, Claremont 7735

We have been assured by our cyber-security consultants that:

- they have identified and addressed the vulnerability; and
- our IT infrastructure is both safe and secure; and
- they have further enhanced our IT infrastructure with security protocols of an exceptionally high standard.

To this end we quote from the assurance given by iSquared:

> *"In response to your query for an assurance as to the security and safety of your IT infrastructure, iSquared is able to confirm that your IT data files are no longer compromised and, as such, your IT infrastructure is safe and secure. We have taken extra-ordinary measures to further enhance your IT infrastructure, which otherwise conformed to best practice, to ensure that your security protocols are of an exceptionally high standard."*

Is information now safe?

We are assured, by our cyber-security consultants, that:

- going forward, our IT systems have been secured and that all information thereon is now safe; and
- we have done all we can to ensure the security of our IT infrastructure and data.

In short: we are assured that going forward information on our IT system should be safe.

How will clients know whether or not they have been affected?

We will update our website with new information as and when it comes to hand.

If, however, a client is made aware of any personal information being released in the public domain, we and the authorities need to know about it so we can have it investigated.

Who can a client contact with any concerns or queries?

We invite clients to contact us on 021 657 5960 or email info@miplan.co.za.

What should a client do?

Our cyber-security consultants recommend that:

- clients change passwords required when dealing with or on our platform; and

www.miplan.co.za

Tel: 021 657 5960 | Fax: 021 657 5970 | info@miplan.co.za
1st Floor, Mariendahl House, Newlands-On-Main, Newlands 7700
PO Box 23271, Claremont 7735

- clients regularly change all their passwords; and

- clients should monitor their inboxes for suspicious looking phishing emails and immediately delete them; and

- clients should monitor their electronic devices for any abnormal behavior or activity and be vigilant at all times; and

- clients should confirm their electronic correspondence to and from us with an in person communication; and

- clients should not click on a link in an email to change their passwords.