**FAQ's**

**General breach-related questions**

1. What is a data breach?

A data breach is an incident in which sensitive, protected or confidential data has intentionally been accessed, viewed, stolen or used by someone who is not authorised to do so. Often, data breaches are committed by criminals trying to steal financial information.

2. When did the breach happen?

Debt-IN became aware that some of our secure servers may have been compromised in April this year. We immediately launched a comprehensive investigation involving both internal and external specialist forensic investigators, with no breach of data detected at the time. It was only in September 2021 that we discovered that personal data from our servers in April had been placed by criminals on hidden websites that are only accessible by specialised browsers.

3. How did Debt-IN become aware of the breach?

One of our partners alerted Debt-IN to the stolen personal data files while doing a routine, highly-focused "sweep" of data posted on a the hidden collection of websites that can only be accessed by specialised browsers. We were able to definitively confirm that the data was the personal information of some 1.4 million consumers on 17 September 2021.

4. How did the breach happen?

This is still the subject of ongoing forensic investigations, and we cannot disclose any details at this stage. We can, however, confirm that the data breach was the result of a malicious criminal attack by external threat actors.

5. When did Debt-IN become aware that there was data leaked?

Debt-IN could make a definitive finding on the evening of 16 September that personal data records had been breached and posted on hidden internet sites that are only accessible by a specialised web browser.

6. What has Debt-IN done to protect customers' information since we became aware that the data had been breached?

Our investigations to date have revealed that the data was likely breached in April 2021. It is quite common for cyber criminals to breach enterprise data systems months before an actual ransomware attack and/or making the data breach known. In recent months Debt-IN has made significant investments in enhanced data security systems and skills. As regards the breach, the company has taken immediate and appropriate actions to reinforce existing security measures and to mitigate any further potential impacts of the breach, including assembling a team of highly regarded and globally experienced cyberbreach and forensic experts to work with Debt-IN on the incident. Debt-IN is working closely with the regulator, law enforcement agencies and other cyber-security partners to rapidly gather facts, resolve the issue and provide ongoing information to clients.

7. What security measures are currently in place to avoid this happening again?

With regard to the breach, the company has taken immediate and appropriate actions to reinforce existing security measures and to mitigate any further potential impacts of the breach, including assembling a team of highly regarded and globally experienced cyberbreach and forensic experts to

work with Debt-IN on the incident. Debt-IN is working closely with the regulator, law enforcement agencies and other cyber-security partners to rapidly gather facts, resolve the issue and provide ongoing information to clients.

8. What type of data has leaked?

While the level of personal details accessed via the breach varies for individual customers, the personal information may include:

- Customer name
- Customer Surname
- Customer contact details (email, mobile and landline)
- Customer ID numbers
- Customer account numbers
- Customer transactional data (balance owed, payment dates, payment amounts)
- Customer Employer information (salary date, employer name, employer address)

9. Is there a possibility that any more data than what we are aware of has leaked?

While the investigations are ongoing and the analysis subject to change, the findings to date show there has been no further breach and enhanced data protection measures remain securely in place.

10. Have you reported this to the regulator and law enforcement agencies?

Debt-IN is engaging with all relevant local authorities and criminal charges have been opened at the South African Police Services. The company has also notified all affected clients.

11. Has the leaked data been published and viewed?

Yes, the data has been posted on hidden websites that are only accessible by specialised browsers. According to our investigations, the data has been the subject of limiting viewing on the these hidden websites, but this is an ongoing investigation and the precise number of views is subject to change. We are engaging with the relevant specialists to see how best to address and resolve the illegal posting of the data.

12. When was the leaked data published?

The leaked personal data was first detected by one of our partners on 14 September.

13. What was the time difference between finding out data was leaked and communicating to the relevant people?

Communication with the impacted clients and the relevant regulators and law enforcement agencies was initiated as soon as we could definitely confirm the authenticity of the published data, which was on 17 September.

14. What efforts have been made by Debt-IN to attempt to take down the leaked data from the published source?

Restoring the integrity of our client's data is an urgent priority for us, but this is a very complex challenge as we are dealing with highly sophisticated cyber criminals and their proxies. Debt-IN has assembled a team of highly regarded and globally experienced cyberbreach and forensic experts to work with Debt-IN on the incident, but at this stage we are unable to provide further information around initiatives to remove the personal data from the websites, given the highly sensitive nature of the case.

15. Who can I speak to about this at Debt-IN for assistance?

0800079661 – call us on this number

compliance@debtin.co.za – email us on this address