Evide
Innovation Centre, Bay Road
Derry - Londonderry, BT48 7TG
T: 00 44 (0) 2871 225 395
Company Reg. No. NI650789

19 May 2023

Dear Customer,

Important – please read carefully.

We write further to our last update on 4 May 2023 to provide a final update in relation to the recent cyber security incident in which we previously informed you that Evide's systems were accessed by an unauthorised third party ("**UTP**").

On 4 May we were able to inform you that your data had not been copied by the UTP. We write now to inform you that our investigations into the incident have now concluded and we set out the findings concerning the incident.

Outcome of our investigations

Our forensic investigation into the incident has now concluded. The report we have obtained from the external IT consultants is confidential and subject to legal privilege however we are able to set out the key findings about the incident.

In summary, there is no evidence that any user or admin accounts were compromised to carry out the attack. Evide's own software, Impact Tracker, was also not compromised. Rather, the UTP was able to send queries directly to the database server via the software used to run the server. The software is provided by the company that hosts our servers. This led to the UTP to submit a "mysqldump" request, a request normally used for legitimate purposes, when transferring databases. This could be done without compromising an account or deploying malware on the server itself. As such, no accounts were compromised and this version of the software has been removed.

After the transfer of some data all database files were deleted from the server by the same method. Evide were however able to recover the databases from available backups.

There is no evidence that the separate Evide document server was compromised at any time during the incident. There is also no evidence of persistent access being maintained by the UTP.

Our investigation has also led us to conclude that the UTP was able to exfiltrate a subset of the data only. This affects less than a dozen clients, rather than the entirety of our client base.

We confirm that no ransom was paid to the UTP.

Next steps

Since the incident occurred back-up data was restored to a clean server and software being run on the server has been checked to confirm that it is the latest stable release. We have installed additional sophisticated software, recommended by our cyber security experts, to monitor the system. Nothing of concern has been detected. Based on the above steps Evide's and its forensic IT investigators have confirmed that, while absolute guarantees can never be given, they are as sure as they can be that the new systems are secure.

We are continuing to invest and enhance our systems and are taking all measures practically possible to prevent this occurring again. In particular we have implemented the following or are in the process of developing:

- **Two Factor Authentication, or 2FA**: We are currently in the process of developing 2FA implementation to Impact Tracker. 2FA is an extra layer of protection used to ensure the security of online accounts beyond just a username and password.

Evide

Innovation Centre, Bay Road

Derry - Londonderry, BT48 7TG

T: 00 44 (0) 2871 225 395

Company Reg. No. NI650789

- **Field Level Encryption**: We are currently in the process of developing/implementing field level encryption to Impact Tracker's database. This will entail 256 bit encryption of key identifiable information (e.g. Name, address, email etc) that will anonymize the data without the correct encryption keys. The keys are stored on the code server, separate from the database server ensuring that decryption cannot occur without both parts.
- **Cloudflare/Atomic Processor:** Cloudflare is currently implemented but has some potential performance drawbacks. As such we are evaluating other tools such as Atomic Processor. Both feature compliance and vulnerability management, reporting, intrusion prevention, file integrity monitoring, memory protection and exploit prevention, vulnerability shielding, web application and API protection, application control, and more.
- **Cyber Essentials Certificate:** Cyber Essentials is an effective, UK Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.
- **Server hosting platform:** We are currently re-evaluating our server hosting platform and services moving forward with best practices in server maintenance and security at the forefront of any decisions made.
- **Reviews:** We are carrying out reviews to ensure that all our operations consistently adhere to best practices

Please accept our deepest apologies for any inconvenience or concern this incident might have caused you. While we do not plan to issue any further general updates now that the investigation has concluded we remain available to assist with any ongoing queries in relation to the incident. Thank you again for your continued support and patience throughout this matter.

Your sincerely

Niall O'Doherty

Company Director

Evide