



GrowthInvest, Warnford Court, 29 Throgmorton Street, London EC2N 2AT
t: 0300 303 0037 e: enquiries@growthinvest.com

GrowthInvest Initial Statement on Mainspring Data Breach – 18th July 2022

This statement is intended to provide an initial statement and update to a reported data breach at Mainspring Nominees Limited ("Mainspring") and may have already been communicated to advisers and clients. Mainspring is the custodian for a number of the funds that are available on the GrowthInvest platform, mainly EIS, SEIS and IHT funds. If your clients are invested in any of these funds, either via the GrowthInvest platform or directly, it is possible that their data has been accessed and compromised.

Mainspring have created a specific page for anybody who may be affected by the data breach, and which they assure us will be the best way to keep up to speed with the very latest news and updates on this. This page can be found here <https://www.mainspringfs.com/data-notice>

We know that many fund managers and financial advisers have already communicated to their clients, so we are not intending to send any specific communication to any advised clients at this stage, though are very happy to discuss any specific requirements with financial advisers.

Please be assured that the GrowthInvest platform is not directly affected by this data breach and is protected against this type of attack. We take the security of client data extremely seriously and we are doing everything possible to discover how this happened, and to work with Mainspring to get to the bottom of it.

We do recommend that every client and adviser take certain steps to limit the possibility of any further impact and have outlined these in some more detail below, along with initial answers to other key questions.

Background

On the morning of 12 July 2022, Mainspring's threat detection software identified that there was suspicious activity within Mainspring's core IT system. Mainspring's cybersecurity analysts began inspecting the activity and when it was evident that the activity was malicious the system was locked down to contain the attack and prevent further damage. Subsequently, it was determined that ransomware had been installed on various servers within the system. Files across the system had been encrypted with the ransomware and had therefore become inaccessible. As you are probably aware, ransomware is a type of malicious software designed to deny a user or organisation access to files on their computer. Sometimes a request for payment, 'i.e. a ransom', is then made, in exchange for unlocking the files.

In response, Mainspring took immediate steps to contain and investigate the incident. Importantly, we understand that Mainspring has been able to restore all of the data it holds, including yours and your clients', from back-ups, and that it should be back to a normal operational service shortly. There has been no material delay to any necessary processing of data during this period.

Who is Mainspring?

Mainspring is one of the leading independent UK fund administrators and custodians, servicing over 80 fund managers with assets under management of over £8 billion. They provide market leading expertise in fund administration, accounting, operations, reporting and investing. They are headquartered in London and authorised and regulated by the Financial Conduct Authority (FCA).

Which Funds and Fund Managers have been affected?

Mainspring works with a growing number of fund managers in the EIS, SEIS and IHT space, including, but not exclusively:

- Mercia
- Time Investments
- MMC Ventures
- Haatch
- Praetura Ventures
- Regenerate
- VGC Partners
- Parkwalk
- Committed Capital
- Fuel Ventures
- Molten Ventures

If your clients have investments with these fund managers, whether or not they are through the GrowthInvest platform, it is likely that you and your clients will be receiving a communication from them, if this has not already happened.

What information and data was involved or accessed?

Mainspring is working hard to establish precisely what data may have been accessed or taken in the attack. Based on their initial findings they believe it is possible that some advisers' and investors' personal information may have been compromised by the attacker.

- **Adviser information:** The information relating to you as an adviser which Mainspring holds is information that is generally publicly available via the FCA's website, such as the adviser's name, company name and address. It is also possible that corporate bank account information could be contained
- **Investor information:** The personal information of clients which Mainspring holds typically includes the investor's name, address, date of birth, email address, bank account details, national insurance number, and tax IDs.
Please note: that as a client of GrowthInvest, it is likely that in most cases it will be the GrowthInvest bank account details that are supplied. However, Mainspring will have carried out their own AML checks on individuals and stored personal information accordingly.
- **Login credentials:** For accessing Mainspring- supplied fund manager portals
If separate, login credentials (including username and password) have been provided to access individual fund manager portals, it is possible may also have been impacted by the incident for both you as an adviser and your clients. Please note:
 - This is not relating to any login credentials on the GrowthInvest platform, only separate fund manager portals.
 - Not all the Mainspring fund managers will have a portal provided by Mainspring, as some will use a 3rd party, or have built their own.
 - This only applies for advisers or clients who have been given specific access to a Mainspring fund manager portal. For the majority of new investments made through the GrowthInvest platform, we believe that advisers and clients would not generally register or login, preferring to centralise all information on the GrowthInvest portal.

What is the potential Impact on clients?

This is still being assessed. We would like to be very clear that Mainspring has assured GrowthInvest that there has been no impact to any of the client money or assets that they hold. In addition, there is no indication that there has been any attempt to gain unauthorised access to client money or bank accounts or to fraudulently orchestrate payments from them. This is because the area impacted by the security incident was isolated to Mainspring's file servers, where client documents are stored; the core custody and accounting systems were entirely unaffected by this incident.



GrowthInvest, Warnford Court, 29 Throgmorton Street, London EC2N 2AT
t: 0300 303 0037 e: enquiries@growthinvest.com

Please be assured that the GrowthInvest platform has not been directly affected by this data breach, and is protected against this type of attack with multiple layers of security. We take the security of client data extremely seriously and we are doing everything possible to discover how this happened, and to work with Mainspring to get to the bottom of it. Any connections or data exchange mechanisms between GrowthInvest and Mainspring are entirely secure, ringfenced and unaffected by these events.

What are GrowthInvest doing?

We take data privacy and data security extremely seriously and have already set up our entire platform infrastructure to minimise the chances of an attack such as this being successful. In the light of the Mainspring incident, we can confirm the following:

- We are continuing to liaise closely with Mainspring will keep you updated as appropriate.
- We have contacted, or will be contacting, all affected fund managers to ensure that they have sent out the appropriate notices to any clients that may have been affected.
- We have flagged the attack to our main GrowthInvest platform custodians to ensure that they are fully aware, and are taking all measures to monitor for any suspicious activity.
- Our GrowthInvest servers are automatically updated with any security updates as part of “business as usual” processes.
- We have completed additional investigations for any sign of suspicious logins and other activity across all our systems. We can confirm that no issues were found, nor malware detected.
- We already undertake an external review of our cyber-security measures on a regular basis as part of our business as usual processes
- With immediate effect we reserve the right to carry out additional diligence checks on any investor requests. This may include call-backs to advisers.
- Mainspring has notified Action Fraud (the UK cyber police).

What steps can you take to protect yourself and your clients?

Whilst matters remain uncertain, there are steps that you can take to protect you and your [clients](#) and we believe it is advisable to ask your clients:

- Be vigilant: Remain alert to suspicious messages on emails or text messages or any incoming telephone calls. You may wish to ask them to check in with you as an adviser in advance of responding to any such messages.
- Change any relevant passwords, especially on fund manager portals, replacing them with strong and unique passwords
- Monitor bank accounts for unexpected activity. If you notice anything unusual, please refer to [The National Cyber Security Centre guidance](#)



GrowthInvest, Warnford Court, 29 Throgmorton Street, London EC2N 2AT
t: 0300 303 0037 e: enquiries@growthinvest.com

GrowthInvest Communications:

All email communication from GrowthInvest will come from an email with the domain @growthinvest.com. It will most usually be from clientservices@growthinvest.com

We will only ever ask you to send documentation to:

GrowthInvest Warnford Court, 29 Throgmorton Street, London, EC2N 2AT.

We will usually request that it is sent by Royal mail registered delivery.

If either you or your clients wish to check the validity of any communication, this can be done by calling into 0300 303 0037 and asking to speak to a member of the Client services team.

Additional Information and Next Steps:

As per the above, we understand that the investigation is ongoing and that Mainspring will continue to keep their [dedicated data notice page](#) up to date.

We will continue to liaise closely with Mainspring about the incident, and as soon as we have anything further to impart, we will of course update you. Should you have any questions in the meantime, please do not hesitate to email us on clientservices@growthinvest.com or contact us on 0300 303 0037.