FINALSITE

655 Winding Brook Drive
Glastonbury, CT 06033 l USA

MEMORANDUM

To: Finalsite Clients
From: Jon Moser, CEO
Date: January 10, 2022
Re: Statement on Forensic Investigation

The safety and security of our clients' data is of the utmost importance to Finalsite, to our clients, and to the families we serve. The Finalsite team monitors our global network systems 24 hours a day, seven days a week. On Tuesday, January 4, 2022, our team identified the presence of ransomware on certain systems in our environment. We immediately took steps to secure our systems and to contain the activity, including proactively taking systems offline.

We quickly launched an investigation into the event with assistance of third-party specialists, including data privacy attorneys at Mullen Coughlin LLC, and cyber forensic investigators at Charles River Associates. In parallel, we started rebuilding our platform in a new, clean environment. At this time all systems are back online in a secure environment which is being closely monitored.

Below is a summary of the forensic investigation to date:

- We have determined who the threat actor is;
- We have achieved containment of threat actor activity;
- We know that the threat actor entered Finalsite systems on Tuesday, January 4, 2022; and
- We know how the threat actor gained access into our systems.

At this time, based on six days of investigative work, we have found no evidence that client data has been viewed, compromised or extracted.

The investigation is still underway and could take weeks before completion. The remainder of the investigation is to confirm these findings and ensure compliance with applicable laws. Should there be variance in our findings through the remainder of the investigation, we will promptly inform clients and take appropriate next steps. We will inform you when the investigation has been completed and will provide additional information at that time should it be relevant.

Sincerely,

Jon Moser
Founder & CEO
Finalsite

Rebecca Jones
Partner
Mullen Coughlin LLC

Frequently Asked Questions

Q: Who is conducting the investigation?
A: The forensic investigation is being led by cyber criminal investigators at Charles River Associates who are working very closely with Finalsite.

Q: Can you tell us what type of ransomware was used?
A: While we have identified the type of ransomware at issue, we are not able to share this information at this time.

Q: Has any client data been compromised?
A: After six days of investigation, we know when the threat actor entered, how they entered, and what they looked at. We are confident in saying that no client data has been viewed, compromised or extracted. During the remaining course of the investigation, if we determine otherwise, we'll act swiftly to notify you and take appropriate action.

Q: What kinds of data are stored in the Finalsite systems?
A: Primarily, data and files stored by Finaliste are publicly-facing information found on school and district websites.

Clients who use Directories or Messages/eNotify modules will also have demographic data also stored in the Finalsite database, such as names, email addresses and phone numbers.

Some clients use Finalsite payment integrations with third-party organizations. These payments are processed through a secure third-party. **Finalsite does not transmit or store any credit card data**.

Finalsite does **not** store academic records, social security numbers or any other confidential information.

Again, Finalsite has no evidence that **any** data was compromised as a result of this incident.

Q: What security measures are you taking to ensure this doesn't happen again?
A: No organization is immune to ransomware incidents, including even the most secure and advanced technology companies like ours. Finalsite dedicates an extraordinary amount of time and resources to security and is always improving our tools and processes as we learn more about cyber security and how it could impact us and our clients.

Following this event, Finalsite will be making adjustments to its security measures. Revealing all of the steps being taken would be counterproductive and potentially compromise the security of our products and data.

Q: Can you share a timeline for the incident and what occurred?
A: The threat actor accessed the Finalsite system on January 4. This is the same date the issue was discovered and addressed. We can share a more thorough timeline upon the investigation's completion.

Q: Will you be sharing the full investigative report with us?
A: We will inform clients when the investigation is complete, however no new information is expected to be shared at that time unless there is variance in our findings expressed in this document.

Q: Why did you wait two days to inform clients of the situation?
A: Due to the nature of this being a ransomware attack, we were unable to share more information about it with clients right away. We engaged data privacy counsel to guide us through the investigation and response of this incident and ensure compliance with applicable laws.

Many organizations who have been through similar situations delay response to clients and the public by weeks and months, and some never reveal what happened at all. Finalsite is committed to transparency and shared as much as we could, as soon as we could.