Dear [\_\_\_\_\_\_\_\_\_\_\_\_\_\_].

We are writing to you because of a recent incident involving a Birchview Capital, LP (the “Firm”) email account that was accessed by an unauthorized third party. The Firm has investigated this incident and fortunately we have found nothing that indicates there has been any misuse of any of your personally identifiable information. Nonetheless, we felt it important to provide you and certain other potentially affected parties with the courtesy of this notice that will summarize the incident and the precautionary and remedial steps the Firm has taken in response thereto. This notice also includes information in connection with several steps you can take to protect yourself against identity theft or fraud, should you desire to do so.

**The Incident**

On September 26th, the Firm learned that on the prior day, September 25th, a third-party bad actor (the “Attacker”) successfully compromised the Firm email account of one of our team members. That team member was travelling at the time of this unauthorized access and accessed the public wifi internet services provided by an airport. The Attacker was able to temporarily access this employee’s Firm email account and was able to initiate an outbound email to a Firm client, effectively impersonating the employee. We have been in touch with the client who received this email. [All unauthorized access to the Firm’s email accounts was successfully terminated as of \_\_\_\_\_\_.]

**The Firm’s Response and Remedial Actions**

We [immediately/promptly/directly] engaged with several cybersecurity advisors to assist the Firm in not only determining the severity of this situation but also to conduct an investigation of this incident and advise the Firm on evaluating how to respond appropriately, if at all. The investigation included the following:

[PLEASE HAVE VERTEK EXPLAIN EXACTLY WHAT THEY DID. I ASSUME SOME OR ALL OF THE FOLLOWING MAY APPLY

* a full audit of the Firm’s computer network;
* an evaluation of all Firm email accounts and a review of the related access logs;
* termination of all unauthorized access to the subject email account; ]

The investigation revealed that the Attacker did have temporary access to the subject email account but fortunately, we found no evidence that any information had been copied, stolen, acquired or otherwise transferred from the Firm by the Attacker.

Following the investigation, the Firm took the following remedial steps to enhance its security measures: [Please insert any enhancements the Firm took (as alluded to in the email from Jack to Karl dated Oct 23)]. The Firm also alerted certain third parties, including the [Vermont Attorney General].

**Preventative Steps For You to Consider**

Although our investigation did not reveal any evidence indicating that any information residing on the Firm’s network and/or its systems was downloaded, transferred or otherwise taken in this attack, we felt it was important to send this notice to you. At a time when all businesses face numerous aggressive cybersecurity threat vectors, these attacks are commonplace in our industry. Nonetheless, we would recommend that you consider taking certain steps to protect yourself from the possibility of identity theft, such as changing your passwords and security features across your online accounts, reviewing your banking and credit card statements and report any suspicious activity to the relevant issuers and perhaps even contact your credit or debit card company and inform them that your card information may have been compromised, so that they can issue you a replacement card.

If you have any questions or concerns, please do not hesitate to contact the Firm at [\_\_\_\_\_\_\_\_\_\_].