HANNIBAL industries inc.

3851 S. Santa Fe Ave. Los Angeles, CA 90058 323-588-4261 fax 323-589-5640

May 31, 2019

RE: NOTICE OF POTENTIAL DATA BREACH

Dear Valued Partner of Hannibal Industries Inc.:

The purpose of this letter is to provide notice that Hannibal Industries, Inc. ("Hannibal"), discovered that an unauthorized party gained access to Hannibal's computer servers. Hannibal takes your privacy very seriously. We are writing to make sure that you are aware of the issue and the steps we are taking to help protect your personal data.

What Happened?

During the afternoon of Memorial Day, Monday, May 27, 2019, Hannibal became aware that an unauthorized party accessed data stored on Hannibal's servers. A third party remotely took over our server, including the data on the server, and our website. This third party is currently asking Hannibal for money to release its control over the server, data and the website. A data breach in which the data is held for ransom is not the same as a ransomware attack. Ransomware generally restricts access to the data on infected machines until the ransom is paid. A data breach however is a security incident in which sensitive or confidential data is copied and stolen from the organization. **At this point, Hannibal has not discovered any evidence that any data was removed from our servers or otherwise compromised.**

What Information Was Involved?

Hannibal is working diligently to determine the scope of the unauthorized access. We are still in the process of determining what information was involved, so at this point we cannot rule out the possibility that personal information, such as names, addresses, social security numbers and birthdates, were accessed without authorization.

What We Are Doing.

Once we became aware of the unauthorized access, we took a number of actions to determine the nature and scope of the issue. Within hours of discovering the incident, we employed an experienced data security IT firm to immediately secure the system to prevent any additional harm. We then notified law enforcement and are coordinating with their investigation. We retained a law firm who specializing in handling data breach incidents.

We are also taking steps to improve our data security and protect personal information stored on our servers. We continue to monitor our computer systems to identify any other suspicious activity. We are also working with our data security

consultant to enhance our systems with new security measures to detect and prevent any further unauthorized access to our server data.

We are setting up a temporary website at www.Hannibalindustries.com to provide you with information about the incident in a timely manner. If you would like to receive email updates about the incident, please send an email to president.hii@outlook.com confirming your request. If you wish to cancel your request that we communicate with you via email on this and other matters, please send us an email opting out of such further communications.

What You Can Do. Because we have no reason to believe that any data was removed from our servers, there are no immediate actions you need to take to protect data stored in our system. However, if you would like to learn how to prevent this type of issue from affecting your own systems, please review the enclosed memo regarding "Safe Email Practices".

For More Information. Call (323) 894-5599 to leave a message on our telephone server and we will respond to any questions you may have.

Please feel free to contact Hannibal directly if you have any questions.

Very truly yours,

Blanton Bartlett

President

Enclosure

Swift Chip

Safe Email Practices

Why?

Unsafe computing can corrupt your files, expose the contents of your internal drive to strangers, cause other computers to become compromised, and even allow your computer to be used by spammers to send millions of unsolicited emails.

Using safe email practices helps you:

- **Protect your inbox**
- **Protect your computer**
- **Protect your privacy**
- **Protect your friends and neighbors**

Here are recommendations you should follow to protect yourself when using email.

1. Screen messages before viewing them, and delete anything that appears suspicious.

1. **Carefully examine your list of unopened messages.**
   Do any of them come from people or addresses you don't recognize? Do the subject lines have words with too many spaces, or long random numbers? Do they seem too good to be true, or somehow odd? If so, it's probably best to just delete the message along with any attachments.

2. **Wait! Don't open that email yet...**
   If a message has attachments don't open it unless you know the sender and are expecting the attachment. If you're not sure what it is, contact the sender before opening the message and ask exactly what the message and attachment is.

3. **Don't be fooled by Dirty Tricks.**
   Most computer worms (a kind of malicious program) spread themselves via email by spoofing addresses found in the infected computer's address book and sending copies of itself to other addresses in the address book, so it's very likely that an infected message can appear to come from someone you know. Many of these messages will use vague or generic subject lines like "Re: " or "Hi." Others will try to look like they come from a technical support service, or even from Microsoft. Be careful about opening these.

4. **Always confirm a Wire Transfer.**

   An extremely common attack we are seeing is for an email to come in that appears to be from a user in the company. If the email address matches exactly, this is called “spoofing.” Also check to see if the domain name is slightly off. For instance, instead of “gmail.com” it says “gmaii.com.” These emails often request a wire transfer, and are targeting accountants and CFOs. Please verify with the person directly.

2. Open your messages, but beware the Next and Previous buttons.

Using the Next and Previous buttons to open and move from message to message is convenient but dangerous, especially if you don't screen messages thoroughly, or if new messages come in while you're reading other screened messages.

3. Handle Attachments Safely.

- **Don't open attachments unless you are absolutely sure about what they are and who they came from.**
  Even attachments that were sent directly to you by a known sender might contain malicious code.
- **Be especially careful with MS Word & Excel files.**
  When opening Microsoft Word or Excel attachments containing macros, always select the "Disable Macros" option if you are not sure if there should be a macro.
- **Beware of Dangerous File Types!**
  Some file types have been deemed unsafe by Microsoft. Most of these file types are executable or exploitable and are considered unsafe to send and receive as email attachments. SSU's email servers scan all incoming email messages for attachments using these unsafe file types. If you also use an off-campus email address, you should be aware of these unsafe file types. Never open zip files, exe files or one of these unsafe file types sent in email. While many of these file types can only harm computers running Windows, some file types are potentially hazardous on Macintosh computers.
- **Windows Users - Make Extensions Visible**
  Some malicious attachments will "pose" as a harmless file type like digital image by including that file type extension in its name. You might get an attachment called "hawaii.jpg" and think it's a picture from your friend's vacation. But it might actually be a .pif file, one of the exploitable file types. This can happen because Windows does not display file extensions by default, so a .pif file named"hawaii.jpg.pif" will appear as "hawaii.jpg"

4. Don't Unsubscribe.

Spammers often include an "unsubscribe from this list" link in their messages. This makes them appear more responsible and reputable, but they often use this as a way to confirm your email address so they can send you more spam or sell your email address to other spammers. If you don't want it, mark it as junk and delete it.

Swift Chip

5. Be a Good Internet Citizen.

- Don't use your email in ways that will contribute to the problem.
- Don't send unsolicited email and attachments.
- Don't forward chain letters.
- Don't respond to or participate in email hoaxes.
- Don't send attachments which use the "unsafe" file types.
- Don't post your email address (or other people’s addresses) on publicly accessible web pages.
- Use a "disposable" email account (a free account from yahoo or hotmail) for online shopping and posting to online discussion boards.