Clark Hill

Jason M. Schwent
T (312) 985-5939
F (312) 517-7573
Email:jschwent@ClarkHill.com

Clark Hill, PLC
130 E. Randolph Street,
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

July 15, 2021

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Dear Attorney General Frey:

We represent Computer Information Concepts, Inc. ("CIC") with respect to a data security incident involving the potential exposure of certain personally identifiable information ("PII") described in more detail below. CIC is an IT, software, and professional services company located in Greeley, Colorado. CIC is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On March 16, 2021, CIC identified suspicious network activity when they were unable to log-in to certain applications and systems in their IT environment. They also identified the presence of ransom notes and encrypted files. With the assistance of Counsel, CIC engaged an independent computer forensics firm to assist with determining what had occurred, the extent of any unauthorized access, and whether any data, including PII, had been compromised or exfiltrated. The investigation determined that CIC had suffered a PYSA ransomware attack and that during the attack an unauthorized individual may have accessed and/or taken files containing a limited amount of PII. On June 1, 2021, the investigation determined that files containing names and Social Security numbers for a limited number of CIC employees and CIC customers may have been impacted.

2. Number of residents affected.

Fifteen (15) Maine residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on July 15, 2021 (a copy of the form notification letter is enclosed).

3. Steps taken or plan to take relating to the incident.

CIC took steps to address this incident and prevent similar incidents in the future. CIC completely restored its environment from clean backups, implemented a global password reset, disabled RDP remote access, required secure VPN access for all remote connections, audited all accounts to ensure stronger password authentication was implemented, and deployed active threat hunting and monitoring software tools. CIC entered into long-term threat hunting and monitoring services with an outside consulting company who are experts in digital forensics and incident response. CIC is also in the process of implementing multi-factor authentication and retraining its employees on recognizing and responding to suspicious computer activity. Finally, impacted individuals are able to enroll in 12 months of credit monitoring and identity restoration services at no cost.

4. Contact information.

CIC takes the security of the information in its control seriously and is committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Very truly yours,

CLARK HILL

JASON M. SCHWENT

Cc: Logan Parker

Enclosure