

January 7, 2022

**VIA OVERNIGHT DELIVERY AND EMAIL DELIVERY TO:
IDTHEFT@OAG.STATE.MD.US**

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

Attention: Security Breach Notification

Re: Notice of a Cybersecurity Event by ETI Technologies, Inc.

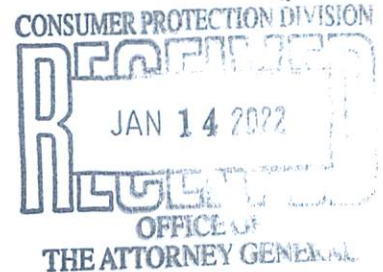
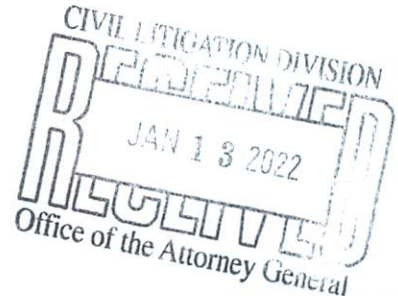
To Whom It May Concern,

This letter shall serve as notice to the Office of the Maryland Attorney General on behalf of our client, Ebara Technologies, Inc. ("ETI" or the "Company") of a network security incident that may have involved personally identifiable information ("PII") of Maryland residents.

On or about November 10, 2021, ETI and its affiliated companies experienced a network security incident, which resulted in the potential compromise of a portion of ETI's IT environment. The incident was first discovered on November 10, 2021, when employees of ETI were "locked out" of the ETI IT network environment. Immediately upon learning of the incident, ETI took steps to contain the incident and conduct a thorough investigation. ETI retained a third-party forensic and cyber security IT firm to assist in the remediation of its system, including eliminating the vulnerability that was used by the threat actor and the implementation of additional security measures.

Based on the Company's investigation, it appears the threat actor may be one that is known as Hello Kitty. ETI was able to restore its systems through available backups and no ransom or other extortion payment was made to the threat actor.

ETI has undertaken significant effort to assess the nature and scope of any threat actor access or exfiltration of any PII. Among other things, ETI and its forensic experts analyzed the Company's datasets that contain PII to determine whether there was evidence by which the



VIA OVERNIGHT DELIVERY AND EMAIL DELIVERY TO:
IDTHEFT@OAG.STATE.MD.US

Company could reasonably conclude that the threat actor did not have access to and/or did not exfiltrate data. While ETI has been able to conclude that most datasets were not compromised by the threat actor, on or about December 13, 2021, ETI determined that it was unable to fully exclude certain limited datasets due to the absence of sufficient forensic artifacts to conclusively rule out access or exfiltration.

Accordingly, in an abundance of caution, for those datasets that could not be reasonably excluded, ETI will be notifying all individuals whose PII is present. One of those datasets included PII of current and former ETI employees and their respective dependents. ETI is in the process of notifying these affected individuals about the network security incident.

The types of PII that may have been impacted for all affected individuals include:

- Social Security Number
- Driver's License Number
- Health care and other medical information; and
- Forms of identification that may include a driver's license, passport, or other ID number.

We have included the templates that are being used to notify these individuals of the network security incident and anticipate that affected individuals, whose number to date is approximately nine (9) from your state, will receive these notices on or about January 10, 2021. The Company will also provide these individuals with twenty-four (24) months of credit monitoring and identity theft insurance free of charge. To date, the total number of affected individuals for this incident is approximately 1,369.

We will inform you as we learn additional pertinent information about the incident. Any questions about this incident can be directed to me at colin.jennings@squirepb.com.

Sincerely,
Squire Patton Boggs (US) LLP



Colin R. Jennings

cc: Ericka Johnson, Esq.

Attached: Ebara Current Family Employee Notification Letter; Ebara Current Individual Employee Notification Letter; Ebara Former Family Employee Notification Letter; Ebara Former Individual Employee Notification Letter