

# BakerHostetler

## Baker&Hostetler LLP

1170 Peachtree Street  
Suite 2400  
Atlanta, GA 30309-7676

T 404.459.0050  
F 404.459.5734  
www.bakerlaw.com

John P. Hutchins  
direct dial: 404.946.9812  
jhutchins@bakerlaw.com

December 9, 2022

### VIA EMAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

*Re: Incident Notification*

Dear Attorney General Formella:

We are writing on behalf of our client, KEMET Electronics Corporation (“KEMET”), to notify you of a security incident.

On October 11, 2022, KEMET identified a data security incident. KEMET immediately took steps to secure its computer systems and began an investigation with assistance from a cybersecurity firm. The investigation determined that an unauthorized person gained access to some of KEMET’s computer systems on October 11 and October 12, 2022. KEMET further investigated to identify the type of information maintained on the computer systems that were accessed and concluded that they may have contained the names, Social Security numbers, driver’s license numbers, financial account numbers, health insurance enrollment information, and/or limited medical information of eight New Hampshire residents.

On December 9, 2022, KEMET mailed notification letters to the New Hampshire residents via U.S. First-Class mail in accordance with HIPAA (45 C.F.R. § 164.404) and N.H. Rev. Stat. Ann. § 359-C:20.<sup>1</sup> A copy of the notification letter is enclosed. KEMET is offering notified individuals complimentary, one-year memberships to credit monitoring and identity theft prevention services through Kroll. KEMET has also established a dedicated, toll-free call center where individuals may obtain more information regarding the incident.

---

<sup>1</sup> This report does not waive KEMET’s objection that New Hampshire lacks regulatory authority over it related to any claims that may arise from this incident.

December 9, 2022

Page 2

KEMET is enhancing its existing security protocols and technical safeguards and is updating its policies on document retention and sensitive information capture to prevent something like this from happening again.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

John P. Hutchins  
Partner

Enclosure



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

KEMET Electronics Corporation addressed a data security incident that involved some of your information. This letter explains the incident, the measures we have taken, and some steps you may consider taking in response.

On October 11, 2022, we identified a data security incident. We immediately took steps to secure our computer systems and began an investigation with assistance from a cybersecurity firm. The investigation determined that an unauthorized person gained access to some of our computer systems on October 11 and October 12, 2022. We further investigated to determine the computer systems that were accessed and concluded that some of them contained certain personal information.

We determined that some of your personal information may have been involved, including your name and one or more of the following: Social Security number, driver's license number, financial account number, date of birth and limited medical information related to your employment. Further, if you are currently or were ever previously enrolled in our employee health plan, information related to your enrollment in that plan or information about your claims under that plan may also have been involved.

We regret any inconvenience or concern this incident may cause you, and in an abundance of caution, we are offering complimentary identity monitoring services through Kroll at no cost to you for one year. Your identity monitoring services include credit monitoring, fraud consultation, and identity theft restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until <<b2b\_text\_6 (activation date)>> to activate your identity monitoring services.*

Membership Number: <<Membership Number s\_n>>

For additional steps you can take in response to the incident, please see the additional information provided in this letter.

We also encourage you to remain vigilant by reviewing your financial account statements, credit reports, and statements from your healthcare provider and health insurance plan for any unauthorized activity. If you see charges or activity that you did not authorize, please contact the relevant financial institution, credit bureau reporting the activity immediately, or your healthcare provider or health insurance plan provider.

We want to assure you we value protecting your information. We are enhancing our existing security protocols and technical safeguards to attempt to prevent unauthorized access to our systems in the future. Additionally, we are updating our policies on document retention and sensitive information capture in order to attempt to prevent issues like this from impacting KEMET in the future. We have established a dedicated call center to help answer any questions you may have about the incident. Please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays, for up-to-date information about the incident.

Sincerely,

Mike Raynor  
Chief Financial Officer



## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services from Kroll:

### **Triple Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

Fraud Alerts and Credit or Security Freezes:

*Fraud Alerts:* There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

*Credit or Security Freezes:* You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- Experian Security Freeze, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

KEMET's address is 1 East Broward Boulevard, Fort Lauderdale, FL., 33301 and its phone number is (954) 766-2800.

**Additional information for residents of the following states:**

**Maryland:** You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us)

**New York:** You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)

**Rhode Island:** **This incident involves XXX individuals in Rhode Island.** Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, [www.riag.ri.gov](http://www.riag.ri.gov)

**West Virginia:** You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.