Representing Management Exclusively in Workplace Law and Related Litigation

jackson lewis
Attorneys at Law

JASON C. GAVEJIAN
Email Address: gavejiaj@jacksonlewis.com

Jackson Lewis LLP
220 Headquarters Plaza
East Tower, 7th Floor
Morristown, NJ 07960-6834
Tel 973 538-6890
Fax 973 540-9015
www.jacksonlewis.com
Richard J. Cino - Managing Partner

ALBANY, NY
ALBUQUERQUE, NM
ATLANTA, GA
BIRMINGHAM, AL
BOSTON, MA
CHICAGO, IL
CINCINNATI, OH
CLEVELAND, OH
DALLAS, TX
DENVER, CO
DETROIT, MI
GREENVILLE, SC
HARTFORD, CT
HOUSTON, TX
JACKSONVILLE, FL
LAS VEGAS, NV
LONG ISLAND, NY
LOS ANGELES, CA
MEMPHIS, TN
MIAMI, FL
MINNEAPOLIS, MN
MORRISTOWN, NJ
NEW ORLEANS, LA
NEW YORK, NY
OMAHA, NE
ORANGE COUNTY, CA
ORLANDO, FL
PHILADELPHIA, PA
PHOENIX, AZ
PITTSBURGH, PA
PORTLAND, OR
PORTSMOUTH, NH
PROVIDENCE, RI
RALEIGH-DURHAM, NC
RICHMOND, VA
SACRAMENTO, CA
SAN DIEGO, CA
SAN FRANCISCO, CA
SEATTLE, WA
STAMFORD, CT
WASHINGTON, DC REGION
WHITE PLAINS, NY

December 29, 2010

**VIA FEDERAL EXPRESS**
Honorable Michael A. Delaney
Office of the Attorney General
Consumer Protection Division
33 Capitol Street
Concord, NH 03301

Re: Data Breach Notification

Dear Attorney General Delaney:

Please be advised that our client, Heraeus Incorporated experienced a data breach when, on November 18, 2010, it noticed that a steel cabinet which housed a small safe containing tape backups for the Company's IT data and software was missing. After an extensive search, the cabinet, tapes, and safe have not been located. It is believed the cabinet was disposed of along with many other items during a mass cleaning that occurred prior to contractors beginning demolition in the building. The items disposed during this mass cleaning were taken to a transfer station, crushed, and then transported to as landfill in Pennsylvania where they would have been crushed again and then buried.

On the tapes were "images" of each machine stored on separate files. To extract data, you would need to use the software that created the image. On these "images" the following personal information may have been stored: name, address, social security numbers, financial account numbers, driver's license numbers, medical and/or other personal information. It appears that as many as 540 individuals could have been affected, including 1 residents of New Hampshire. Immediately upon discovering this fact, Heraeus took immediate steps to begin an investigation as to what potential information was contained on these "images" and which individuals were potentially impacted. To date, Heraeus has received no information indicating this information has been improperly utilized. Nevertheless, Heraeus plans to begin notifying the affected individuals in the next several days. A draft copy of the notification that will be sent is attached.

As set forth in the attached letter, Heraeus has taken numerous steps to protect the security of the personal information of the affected individuals. Also, in addition to continuing to monitor this situation, Heraeus is reexamining it current data privacy and security policies and procedures to find ways of reducing the risk of future

data breaches. Should Heraeus become aware of any significant developments concerning this situation, we will inform you.

If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS LLP

Jason C. Gavejian

Encl.
4839-3567-3608, v. 1

***DRAFT - General***

**[LETTERHEAD]**

[Date]

[FIRST NAME] [LAST NAME]
[STREET ADDRESS]
[EXTENDED ADDRESS]
[CITY], [STATE] [ZIP]

Dear [FIRST NAME] [LAST NAME],

Please be advised that on or about November 18, 2010, Heraeus Incorporated noticed that a steel cabinet which housed a small safe containing tape backups for the Company's IT data and software was missing. After an extensive search, the cabinet, tapes, and safe have not been located. It is believed the cabinet was disposed of along with many other items during a mass cleaning that occurred prior to contractors beginning demolition in the building. The items disposed during this mass cleaning were taken to a transfer station, crushed, and then transported to as landfill in Pennsylvania where they would have been crushed again and then buried. It is believed that these tape backups may contain one or more of the following – name, address, Social Security number, financial account number, drivers' license number, medical and/or other personal information of individuals.

Immediately upon receiving this information, Heraeus took steps to recover the tape backups, protect its systems and operations, and determine the cause. To date, the tape backups have not been recovered. An investigation of this incident is ongoing.

We apologize for this situation and any inconvenience it may cause you.

We are not aware of any improper use of the personal information contained in the tape backups. Nonetheless, we are sending this advisory to you and other individuals whose personal information may have been contained in the documents to make you aware of this incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information. The attached sheet describes steps you can take to protect your identity, credit and personal information.

While we believe that there is little likelihood your information will be misused as a result of this incident and because protecting your personal information is important to us, we are providing you with a year of free identity theft protection — IDFREEZE™ from TrustedID. This proactive protection is designed to stop any possible identity theft or fraud before it happens. Enrolling in this protection is fast and simple. You can sign up now for a year of protection – again, at no cost to you – at **https://www.trustedid.com/idfreeze/** at this point enter the promo code that was given to you [INSERT] and then hit "**ENROLL**" (this step is very key). Next, enter the necessary personal information to begin your protection. You can sign up for the online or offline identify theft protection service anytime between now and [INSERT]. Unfortunately, due to privacy laws, we cannot register you directly.

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. For questions about the theft protections services described above, you should call IDFreeze at 1-888-880-0761 (pass code [INSERT]). For questions about the incident, or if you detect any signs that anyone has used your personal information without your permission before you registered for this protection, please let us know immediately by contacting [contact person/title] at [number].

Sincerely,
[Name and title]

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

## What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to protect your personal information:

1. Contacting the nationwide credit-reporting agencies as soon as possible to:
   - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Receive a free copy of your credit report by going to www.annualcreditreport.com.

   Equifax
   P.O. Box 740256
   Atlanta, GA 30374
   (800) 525-6285
   www.equifax.com

   Experian
   P.O. Box 9554
   Allen, TX 75013
   (888) 397-3742
   https://www.experian.com/fraud/center.html

   TransUnion
   P.O. Box 6790
   Fullerton, CA 92834
   (800) 680-7289
   www.transunion.com

2. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues and how to avoid identity theft. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local police and you also can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

4. For *North Carolina Residents:* For more information on identity theft please contact either the Federal Trade Commission at the contact information provided above, or North Carolina's Attorney General's Office, Address: 9001 Mail Service Center, Raleigh, NC 27699-9001; Telephone: (919) 716-6400; Fax: (919) 716-6750; website: www.ncdoj.com/

5. *For Maryland Residents*: The contact information for the State's Office of the Attorney General, which provides information about how to avoid identity theft, is

   Honorable Douglas F. Gansler
   Office of the Attorney General
   200 St. Paul Place
   Baltimore, MD 21202

   Website: http://www.oag.state.md.us
   Telephone number: (888) 743-0023
   (toll-free in Maryland)