



Attorneys at Law

Representing Management Exclusively in Workplace Law and Related Litigation

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
BALTIMORE, MD
BIRMINGHAM, AL
BOSTON, MA
CHICAGO, IL
CINCINNATI, OH
CLEVELAND, OH
DALLAS, TX
DENVER, CO
DETROIT, MI
GREENVILLE, SC
HARTFORD, CT
HOUSTON, TX
INDIANAPOLIS, IN
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
NORFOLK, VA
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

July 7, 2010

VIA FEDERAL EXPRESS

Via First Class Mail and Email (oag@oag.state.md.us)

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

Re: Data Breach Notification

Dear Attorney General Gansler:

Please be advised that on or about June 15, 2010, our client, The Knights of Columbus, was notified that a small number of its underwriting files and additional documents containing 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 – was found outdoors near its headquarters in New Haven, Connecticut. Immediately upon receiving this information, the Order took steps to recover the documents, protect its systems and operations, and determine the cause. The files and a significant number of documents have been recovered. However, during the course of its investigation, the Knights of Columbus learned that other underwriting files were not in their designated locations and may be missing from its premises. An investigation of this incident and search for these additional files is ongoing.

It appears that as many as 268 individuals could have been affected, including 5 residents of Maryland. To date, The Knights of Columbus has received no information indicating this information has been improperly utilized. The Knights of Columbus 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, The Knights of Columbus 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, The Knights of Columbus is reexamining its current data privacy and security policies and procedures to find ways of reducing the risk of future data breaches. Should The Knights of Columbus 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

Joseph J. Lazzarotti

Encl.

DRAFT

[LETTERHEAD]

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

Dear [FIRST NAME] [LAST NAME],

Please be advised that on or about June 15, 2010, The Knights of Columbus, was notified that a small number of its underwriting files and additional documents containing 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 – was found outdoors near its headquarters in New Haven, Connecticut. Immediately upon receiving this information, the Order took steps to recover the documents, protect its systems and operations, and determine the cause. The files and a significant number of documents have been recovered. However, during the course of its investigation, the Knights of Columbus learned that other underwriting files were not in their designated locations and may be missing from its premises. An investigation of this incident and search for these additional files 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 documents. 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 have arranged for you to enroll, at no cost to you, in an online 3-bureau credit monitoring service for **[X year(s)]** provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three major nationwide credit reporting companies. To enroll in this service, go to the TransUnion Interactive Web site at **<number>** and in the space referenced as **<Activation Code>**, enter **<Insert Activation Code>** and follow the simple steps to receive your products online instantly.

If you have any questions regarding this incident, are concerned that you may have an identity theft issue, or do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, please call **<number>** Monday through Friday, 9:00 a.m. to 7:00 p.m. Eastern time. Please enter or say the following six-digit pass code **<Insert 6-digit Pass Code>** when prompted. You can sign up for the online or offline credit monitoring service anytime **between now and October 15, 2010**, by using the code listed above. Unfortunately, due to privacy laws, we cannot register you directly. Once you are enrolled the credit monitoring service will notify you if there are any critical changes to your credit files, including fraudulent activity, new inquiries, new accounts, new public records, late payments, change of address and more.

Special note for minors affected by the breach: The same service referred to above may not be available to affected minors. A TransUnion representative at the telephone number above will be able to answer your questions about the services that can be provided to minors. You can access more information at the following site:
<https://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/childIdTheft.page>

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 monitoring services described above, you should call TransUnion at **[800 number]**. For questions about the incident, you should call **[800 number]**.

Sincerely,

Emilio B. Moure
Supreme Treasurer

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
<http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/fraudAlert.page>

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 Maryland Residents:* Under Maryland and federal law, you are entitled to two FREE credit reports from each of the Credit Reporting Agencies each year. Go to www.annualcreditreport.com or call 1-877-322-8228 to access your report through the federal Fair Credit Reporting Act. You must contact each of the three Credit Reporting Agencies individually to access your credit report under Maryland law. The contact information for these Agencies is provided above. 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 or (410) 576-6360
(toll-free in Maryland)

5. *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/
6. *For Massachusetts Residents:* Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit

reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (<https://www.freeze.equifax.com>); Experian (<https://www.experian.com/freeze/center.html>); and TransUnion (<http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/securityFreeze.page#5>) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.