Representing Management Exclusively in Workplace Law and Related Litigation

jackson lewis
Attorneys at Law

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
AUSTIN, TX
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
MILWAUKEE, WI
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
SAINT LOUIS, MO
SAN DIEGO, CA
SAN FRANCISCO, CA
SEATTLE, WA
STAMFORD, CT
WASHINGTON, DC REGION
WHITE PLAINS, NY

Joseph J. Lazzarotti
Direct Dial: (973) 451-6363
Email: lazzarottij@jacksonlewis.com

January 25, 2013

VIA FEDERAL EXPRESS
Via First Class Mail
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Data Breach Notification

Dear Attorney General Delaney:

Please be advised that on January 11, 2013, Fidelity Management Trust Company ("Fidelity") (recordkeeper and trustee for the Plan) reported to my client, Publishers Circulation Fulfillment, Inc. (PCF), instances of unauthorized access and withdrawals of funds from certain participants' accounts under PCF's 401(k) retirement plan ("Plan") suggesting a potential security incident.

There had been an earlier isolated incident involving one person covered under the Plan which neither Fidelity nor PCF believed involved access to the personal information of anyone else in the Plan or at PCF. We believe that incident occurred approximately in July 2012. However, the events leading to Fidelity's January 11, 2013, notice to PCF first occurred on December 24, 2012. The current investigation suggests these incidents may be related.

Upon receipt of Fidelity's January 11, 2013 letter, PCF immediately commenced an investigation and has taken other steps including working with law enforcement, Fidelity and other third parties to determine the nature and scope of the incident. These steps also include changing the process by which Plan participants can access the funds in their accounts. PCF also has filed a report with the state police in New Jersey.

At this point, PCF is aware of a small number of participants who have been affected. However, PCF has not yet been able to confirm how the information was obtained in order to access these accounts, or who might be responsible for these breaches.

In the abundance of caution, PCF has already sent a cautionary email notification to all active users of its information systems, but will be formally notifying all current and former employees who had a Plan account with Fidelity. According to PCF, the number of individuals that potentially could be affected is 1,974 (the number of current and former employees who participated in the Plan), including 15 residents of New Hampshire. However, on January 24, 2013, Detective-Lt. Frank Ramaci of the Bergen County, NJ Police Department requested that PCF postpone the notice of potentially affected persons for approximately two weeks pending his ongoing investigation.

We attach a copy of a draft formal letter that PCF plans to send to potentially affected individuals as soon as Detective-Lt. Ramaci lets us know that doing so will not hamper his investigation. Also, in addition to continuing the investigation and working with law enforcement, PCF is reexamining it current data privacy and security policies and procedures to find ways of reducing the risk of future data breaches. Should PCF 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.

8083
4838-0507-8034, v. 2

502 Washington Avenue
Suite 500
Towson, Maryland 21204

Dear

On January 11, 2013, we learned from Fidelity Management Trust Company ("Fidelity") of a small number of instances of unauthorized access and withdrawals of funds from certain participants' accounts under PCF's 401(k) retirement plan ("Plan"). As you know, Fidelity is the record keeper and trustee for the Plan. The first incident causing Fidelity to believe Plan data might be compromised occurred on or about December 24, 2012. We apologize for any inconvenience this situation may cause you.

Upon learning of this event, PCF immediately commenced an investigation. As part of this investigation, PCF filed reports with law enforcement and has been working with federal, state and local police concerning their investigations, which included delaying this notification to you at the specific request of law enforcement and consistent with applicable law. PCF also has taken other steps including working with Fidelity and other third parties to determine the nature and scope of the incident. These steps also include changing the process by which Plan participants can access the funds in their accounts. During the interim, participants will be required to initiate loan and plan withdrawals with the PCF Benefits Team.

At this point in the investigation, PCF is not yet aware of how the information was obtained in order to access these accounts, nor are we able to confirm the identity of the responsible party(ies). However, we understand that the kind of information at risk is that which would enable a person to access your plan account, which might include your name and Social Security number, and possibly commit other acts of identity theft. We believe the risk is contained to a small group of current and former employees, although, we are notifying you in the abundance of caution to advise you to take appropriate steps to safeguard your accounts and identity. We also enclose an information sheet that describes steps you can take to protect your identity, credit and personal information.

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.

502 Washington Avenue

If you have questions or concerns, you should call PSA's Fiduciary Consulting Group at 410-798-7498 or email them at PCF401k@psafinancial.com.

Sincerely,

Thomas D. Foard
CFO/Exec. Vice President

502 Washington Avenue
Suite 500
Towson, Maryland 21204

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 as your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days. You can also obtain information about fraud alerts and security freezes. See also FTC below.
   - 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	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	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)