YWCA Retirement Fund

Elizabeth S. Clark
Executive Director

November 13, 2007

Office of New Hampshire Attorney General Kelly Ayotte
c/o Consumer Protection Bureau Chief Lauren Noether
33 Capitol Street
Concord, New Hampshire 03301

Re: The Young Women's Christian Association Retirement Fund, Inc. (the "Fund")

Dear Sir or Madam:

This letter is to inform the New Hampshire Attorney General's office about a security breach involving the personal information of Fund participants. This breach is being reported pursuant to the New Hampshire Revised Statutes, Title XXXI, Ch. 359-C, Sect. 359-C:20 (Notification of security breach required). On Monday, October 1, 2007, when the Fund staff arrived at the Fund's office, the staff discovered one computer had been stolen. The stolen computer contained the names and Social Security numbers of individuals who were active participants in the Fund at anytime during the period from January 1, 2002 to September 28, 2007. The stolen computer did *not* contain addresses, account balances, or telephone or email contact points.

Enclosed is a copy of the notice describing the breach sent to the affected Fund participants between October 11, 2007 and October 18, 2007. This notice was distributed to approximately 48 New Hampshire residents.

Please feel free to contact the undersigned at (212) 922-9500, ext. 115, if further information is required.

THE YOUNG WOMEN'S CHRISTIAN
ASSOCIATION RETIREMENT FUND, INC.

By: Elizabeth Clark
Elizabeth Clark
Executive Director

Enclosure

YWCA Retirement Fund

NAME
ADDRESS
CITY, STATE,

October 9, 2007

Personal and Confidential

We are writing to inform you that some of your personal identification information may have been compromised recently. On Monday, October 1 when The Young Women's Christian Association Retirement Fund, Inc. staff arrived at the Fund's office we discovered one computer had been stolen. The stolen computer contained the names and Social Security numbers of individuals who were active Participants in the Fund at anytime during the period from January 1, 2002 to September 28, 2007. The stolen computer did *not* contain addresses, telephone or email contact points and most importantly no account balances. We have every reason to believe this was a crime of opportunity and not intent. Several factors lead us to believe that the risk to your personal data is rather low. There are no guarantees, however, so you must be alert to steps you may want to take to protect against the possible misuse of your personal identification.

Here is further information about what occurred and these facts should help you assess the risk to your personal identification information:

1. only the computer was stolen, not the monitor, not the mouse, not the power pack

2. the stolen computer was of a type that requires a power pack, not a power cord. Power packs are not sold through retail outlets but must be ordered from the computer manufacturer which requires the computer's serial number, the customer's account number and name. Dell has been notified of the theft. Any attempted order will be flagged, the caller id will be recorded and forwarded to both the Fund and the New York Police Department with whom we met Monday afternoon, October 1.

3. a passcode is required to access the personal identification information stored on the stolen computer.

The Fund has reviewed the pertinent 24-hour surveillance tapes from the week-end and they have been turned over to the NYPD. We have already purchased and installed DEFCON cable locks on all computers. In the next few weeks the Fund will consult with a security firm to evaluate our entire operation. It is the intent of the Fund to implement the security firm's recommendations for improving data protection.

We sincerely apologize for causing you concern and work for you may want to take the following actions:

1. Order and review your credit report immediately. You can order a free annual credit report by calling Annual Credit Report Request Service at 1-877-322-8228, or by visiting their website at www.annualcreditreport.com. When you receive a credit report, check it carefully. In particular, check for any accounts that you may not have opened and any inquires from creditors that you did not initiate. Verify your personal information, including address and Social Security number, on the reports. If you see anything incorrect or that you do not understand, contact the credit agency immediately.

   If you find suspicious activity on your credit report, contact your local police or sheriff's office to file a police report regarding identity theft. Maintain a copy of the police report; you may need to provide copies of the report to creditors to clear your records. You can also contact the Federal Trade Commission's Identity Theft Hotline at 1-877-438-4338 if you suspect someone has misappropriated your personal information. For more information on identity theft and on how to protect yourself from fraud, you may visit the Federal Trade Commission's website dedicated to these topics at www.consumer.gov/idtheft.

2. Review all financial account activity often for at least the next 12 months. Promptly report any suspicious activity, including transactions you do not recognize, to the appropriate financial institution.

3. Place a fraud alert or freeze on your credit report. A fraud alert is designed to prevent credit, loans and services from being approved in your name without your consent. This provides an enhanced level of protection; however, it may limit your ability to get immediate credit, including offers available at retail stores. A fraud alert is effective for 90 days and may be removed. In addition some states allow their residents to place freezes on their credit reports. Freezes prevent the sharing of credit report information to most third parties; however; some fees may apply to place a freeze or lift a freeze. All of the three national credit reporting agencies can give you detailed information. Their contact points are:

TransUnion	Equifax	Experian
P.O. Box 6790	P.O. Box 740256	P.O. Box 9532
Fullerton, CA 92834	Atlanta, GA 30374	Allen, TX 75013
1-800-680-7289	1-877-576-5734	1-888-397-3742
www.transunion.com	www.equifax.com	www.experian.com/fraud

Please be assured that we will be ever more vigilant in protecting your data. If you have any questions, or if we may be of any further assistance at anytime, please call us toll-free at 1-800-222-4738.

The YWCA Retirement Fund