

**North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach:	<u>The Young Women's Christian Association Retirement Fund, Inc. (the "Fund")</u>	PLEASE SUBMIT FORM TO: Consumer Protection Division NC Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 Telephone: (919) 716-6000 Toll Free in NC: (877) 566-7226 FAX: (919) 716-6050
Address:	<u>52 Vanderbilt Avenue, Sixth Floor</u> <u>New York, New York 10017</u>	
Telephone:	<u>(212) 922-9507</u>	
Fax:	<u>(212) 922-9511</u>	
Email:	<u>eclark@ywcarf.org</u>	

Date Security Breach Reporting Form submitted: October 24, 2007

Date the Security Breach was discovered: October 1, 2007

Estimated number of affected individuals: 13,000

Estimated number of NC residents affected: 299

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): N/A

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: A computer was stolen that contained the names and social security numbers of 13,000 Fund participants.

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. Yes If so, please describe the security measures protecting the information: See Schedule 1.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: See Schedule 2.

Date affected NC residents were/will be notified: October 12, 15, 16, and 17, 2007

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): See Schedule 3

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))

Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

written notice
 electronic notice (email)
 telephone notice
 substitute notice

Signature: *Elizabeth Clark* **Date:** October 25, 2007
Contact Person, Title: Elizabeth Clark, Executive Director
Address: Same as above
(if different from above)
Telephone: (212) 922-9507 **Fax:** (212) 922-9511 **Email:** eclark@ywcarf.org

SCHEDULE 1
TO
NORTH CAROLINA SECURITY BREACH REPORTING FORM

A passcode is required to access the personal information stored on the computer. The stolen computer was of the type that required a power pack, not a power cord and the power pack was not stolen. These are not sold through retail outlets but must be ordered from Dell which requires the computer serial number and the customer's account number and name. Dell has been notified of the theft and any attempt to order a power pack will be flagged, the caller ID will be recorded and forwarded to the New York Police Department.

SCHEDULE 2
TO
NORTH CAROLINA SECURITY BREACH REPORTING FORM

The Fund has purchased and installed DEFCON cable locks on all computers. The Fund is in the process of engaging a security firm to evaluate its entire operation, and intends to implement the security firm's recommendation for improving data protection.

SCHEDULE 3
TO
NORTH CAROLINA SECURITY BREACH REPORTING FORM

The delay in notification was due to the assessment and evaluation of the extent of the security breach and the determination of the affected participants, legal counsel's review of the notification obligation and the contents of the required notification, and the coordination of the mailing of approximately 13,000 notices to affected participants..

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
P.O. Box 6790
Fullerton, CA 92834
1-800-680-7289
www.transunion.com

Equifax
P.O. Box 740256
Atlanta, GA 30374
1-877-576-5734
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
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.



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: