

CAROLINA MAMMOGRAPHY REGISTRY

UNC-CHAPEL HILL
DEPARTMENT OF RADIOLOGY

CAMPUS BOX 7515
CHAPEL HILL, NC 27599-7515
www.unc.edu/cmrf


* 9 9 9 9 9 9 9 9 * -009
SAMPLE A SAMPLE
123 ANY AVE
ANYTOWN US 12345-6789

September 29, 2009

VIA US MAIL

Dear Ms. SAMPLE A SAMPLE:

I am writing to notify you about a computer security breach that may have resulted in the unauthorized exposure of your personal information. In late July 2009, information technology employees at The University of North Carolina at Chapel Hill (“University”) discovered that a computer server storing data for the Carolina Mammography Registry (“Registry”) at the University’s School of Medicine was targeted in a computer hack. We believe this hacking incident may have occurred in 2007. When University staff learned that the server was compromised, the server was taken down, and all data on the server were removed.

The Registry is a resource for researchers and radiologists who perform mammography. The Registry collects data from radiology practices that provide mammography services and is part of a research project funded by the National Institutes of Health’s National Cancer Institute. Mammography practices participate in order to promote research on breast cancer screening and to compare their results to practices in North Carolina and in six other states. The Registry uses the data provided by mammography practices to advance knowledge about the most effective ways to improve breast cancer detection, understand risk factors, guide future research, and inform policy makers. Additional information about the Registry’s work is available on the Internet at: www.unc.edu/cmrf/ and <http://breastscreening.cancer.gov>.

Unfortunately, some of your personal information was on the Registry’s server at the time of the hacking incident. This information included your name and Social Security number. In many cases, these data also included your date of birth, address, phone number, demographic information, insurance status, and health history information.

Since learning of the server compromise, the University has been conducting an intensive investigation. Despite our investigation, however, we are unable to say for sure whether your personal information was accessed during the hacking incident. Even if your personal information was accessed, we have no way to know whether your personal information has been or will be misused.

As a precaution to protect against identity theft, we recommend that you immediately place a fraud alert on your credit file. A fraud alert advises creditors to contact you before they open any new accounts or change your existing accounts. You may place this fraud alert on your credit file by contacting any one of the three major credit bureaus listed below:

Equifax
1.800.525.6285
PO Box 740241
Atlanta, GA 30374
www.equifax.com

Experian
1.888.397.3742
PO Box 9532
Allen, TX 75013
www.experian.com

TransUnion
1.800.680.7289
PO Box 6790
Fullerton, CA 92834
www.transunion.com

As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your credit file. All three bureaus will then send a credit report to you, free of charge.

Even if you do not notice any suspicious activity on your initial credit reports, the United States Federal Trade Commission ("FTC") recommends that you check your credit reports periodically. Checking your credit reports can help you identify problems and address them quickly. As a precaution, we have enclosed an FTC brochure, "What to Do If Your Personal Information Has Been Compromised," which contains helpful information and references to further resources. Additional information and resources are available from the FTC by visiting their Website, <http://www.ftc.gov/bcp/edu/microsites/idtheft/>, or by calling the FTC's toll-free Identity Theft Helpline at 1.877.438.4338.

Please know that, in addition to contacting you about this incident, we have also notified the mammography practices that participate in the Registry.

As a breast cancer researcher, I have devoted my career to advancing the health of women and working to improve mammography screening, and I am devastated by this incident. Please accept my sincerest apology, and please be assured that the Registry is continuing to evaluate its computer systems and to implement additional measures to safeguard its servers. If you have any questions or concerns, please do not hesitate to contact the University's toll-free call center at 1.877.434.3065. The call center is available to answer your phone call from 9:00 am to 6:00 pm EST Monday through Friday. You can also access additional information about this incident on the Internet at: www.unc.edu/cmr/.

Very truly yours,



Bonnie C. Yankaskas, Ph.D.
Professor, Department of Radiology
Principal Investigator, the Carolina Mammography Registry

Enclosure

FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Division of Consumer & Business Education

What To Do If Your Personal Information Has Been Compromised

Companies or institutions that keep personal information about you have an obligation to safeguard it. Still, from time to time, the personal information they hold may be accidentally disclosed or deliberately stolen. If your information falls into the wrong hands, it may be misused to commit fraud against you.

If you get a notice that your personal information may have been compromised, taking certain steps quickly can minimize the potential for the theft of your identity.

If the stolen information includes your financial accounts, close compromised credit card accounts immediately. Consult with your financial institution about whether to close bank or brokerage accounts immediately or first change your passwords and have the institution monitor for possible fraud. Place passwords on any new accounts that you open. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers.

If the stolen information includes your Social Security number, call the toll-free fraud number of any one of the three nationwide consumer reporting companies and place an initial fraud alert on your credit reports. This alert can help stop someone from opening new credit accounts in your name.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 2002, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

An **initial fraud alert** stays on your credit report for 90 days. When you place this alert on your credit report with one nationwide consumer reporting company, you'll get information about ordering one free credit report from each of the companies. It's prudent to wait about a month after your information was stolen before you order your report. That's because suspicious activity may not show up right away. Once you get your reports, review them for suspicious activity, like inquiries from companies you didn't contact, accounts you didn't open, and debts on your accounts that you can't explain. Check that information — like your SSN, address(es), name or initials, and employers — is correct.

If the stolen information includes your driver's license or other government-issued identification, contact the agencies that issued the documents and follow their procedures to cancel a document and get a replacement. Ask the agency to "flag" your file to keep anyone else from getting a license or another identification document in your name.

Once you've taken these precautions, watch for signs that your information is being misused. For example, you may not get certain bills or other mail on time. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks. Other signs include:

- receiving credit cards that you didn't apply for;
- being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason; and
- getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

Continue to read your financial account statements promptly and carefully, and to monitor your credit reports every few months in the first year of the theft, and once a year thereafter. For more information on getting your credit reports free once a year or buying additional reports, read *Your Access to Free Credit Reports* at ftc.gov/bcp/edu/pubs/consumer/credit/cre34.shtm.

If your information has been misused, file a report about your identity theft with the police, and file a complaint with the Federal Trade Commission at ftc.gov/idtheft. Read *Take Charge: Fighting Back Against Identity Theft* for detailed information on other steps to take in the wake of identity theft.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.



May 2005