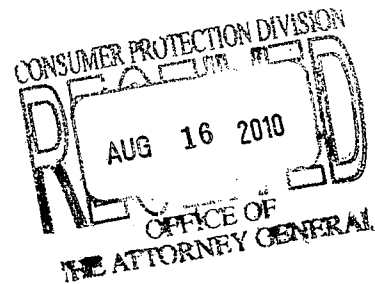




Atlanta Housing Authority



August 13, 2010

Office of the Attorney General
Attn: Security Breach Notification, Hugh Williams
200 St. Paul Place
Baltimore, MD 21202

Dear Mr. Williams:

Pursuant to Md. Code Ann., Com. Law § 14-3501 *et seq.* (the "Notification Statute"), we are writing to inform you that a computer file, which contained certain identifying information about our clients, was inadvertently disclosed to a journalist and a representative from a local advocacy group.

I. Nature of the Unauthorized Access or Use

We recently provided a Microsoft Excel spreadsheet containing statistics about our programs and clients to a journalist writing an article about the Atlanta Housing Authority. After the article was published, a representative from a local advocacy group contacted us requesting the spreadsheet, which we subsequently provided. Soon after receiving the spreadsheet, the advocate informed us on July 22, 2010 that additional information was included. This additional information mistakenly included some of our clients' names, addresses and social security numbers.

II. Number of Residents Affected

Based on our investigation, the inadvertent disclosure included "personal information" of one Maryland resident.

III. Steps We Have Taken or Plan to Take Relating to the Incident

Since learning of the incident, we have taken a number of steps to mitigate its potential impact. First, we worked closely with the journalist and advocate to prevent the possibility that the disclosed information would be further disseminated. Immediately after we learned about the inadvertent disclosure, we confirmed with the recipients that they had not shared any personal information contained in the spreadsheet with anyone else, and that they had destroyed the spreadsheet in its entirety. We want to emphasize that no personal information was included in the article, and we are currently not aware of any evidence that the spreadsheet and related data has been or will likely be used for any fraudulent purpose.

Second, we examined the spreadsheet as well as the events that led to its disclosure. We were able to identify which clients' personal information was included in the spreadsheet, and the underlying circumstances surrounding the disclosure. We also determined that the implicated personal information was not immediately apparent on the opening worksheet,

The Housing Authority of the City of Atlanta, Georgia

230 John Wesley Dobbs Avenue, N.E. • Atlanta, Georgia 30303-2421 • Phone: 404.892.4700 • www.atlantahousing.org

Mr. Hugh Williams
August 13, 2010
Page 2


but was instead included on other worksheets and required a user to explore various tabs within the spreadsheet to locate it. We are currently developing more refined handling processes to prevent a similar breach of this nature in the future, and will be providing additional training to our employees regarding the proper treatment of personal information.

Third, in compliance with the Notification Statute, we will notify the identified state resident by sending a written letter by August 20, 2010 to the last-known address. A sample of the letter is enclosed.

Finally, we have staffed an AHA-internal call center to answer any questions from clients about this incident.

For any information related to this matter, please call me at 404-817-7293.

Sincerely,



Gloria J. Green
General Counsel and Chief Legal Officer

Enclosure



August __, 2010

[Name
Address
City, STATE]

Dear _____ :

This letter is to inform you about an inadvertent disclosure of certain personal and confidential information from a computer file at the Atlanta Housing Authority (AHA). Recently, a confidential computer file containing statistics about AHA's programs and clients were provided to two persons outside of AHA. The file also included your name, address and social security number.

After learning about the disclosure, we immediately confirmed with both people who received the computer file that they did not share any personal information in the file with anyone else. We also confirmed that they have destroyed the entire computer file. Additionally, we have identified the specific circumstances that contributed to this incident and have taken strict measures to prevent future incidents of this nature. At this time, we have no reason to believe that your personal information has been used or will be used improperly or to attempt identity theft.

As a general consumer protection measure, I recommend that you periodically review your credit report and account statements, even if you do not initially find suspicious activity. I have attached to this letter an explanation of additional steps you may consider taking to protect yourself further. As a reminder, you should not release personal information to others unless you are certain of the requester's identity and, as always, you should remain vigilant for incidents of fraud and identity theft.

AHA takes its responsibility to protect your privacy very seriously, and regrets that this incident occurred. If you have any questions about this incident or this letter, please do not hesitate to call Elon Osby at 404-817-7329 or 1-888-AHA-4YOU.

Sincerely,

Barney Simms
Senior Vice President and Chief External Affairs Officer

IDENTITY THEFT PRECAUTIONS

1. Free Credit Report

The Fair Credit Reporting Act requires each of the three nationwide consumer reporting agencies (Equifax, Experian and TransUnion) to provide you annually, upon request, with a free copy of your credit report. Obtaining a copy of your credit report from each agency on an annual basis, and reviewing it for suspicious activity, can help you spot problems and address them quickly. You can request your free credit report online at www.annualcreditreport.com or by telephone at 1-877-322-8228. You can also request your free credit report by completing the request form available at www.ftc.gov/credit, and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

2. Fraud Alert

As a precaution against identity theft, you can consider placing a fraud alert on your credit file. A "fraud alert" tells creditors to contact you before opening a new account or changing an existing account. A fraud alert also lets your creditors know to watch for unusual or suspicious activity. To place a fraud alert, call any one of the three major credit bureaus listed below. An initial fraud alert remains effective for ninety days, and is free of charge. If you wish, you can renew the fraud alert at the expiration of this initial period. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file.

3. National Consumer Reporting Agencies

You can contact the three major consumer reporting agencies at the following numbers and addresses to place a fraud alert and to report fraud:

Equifax

P.O. Box 740241
Atlanta, GA 30374
Toll-free: 800-525-6285

TransUnion

Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
Toll-free: 800-680-7289

Experian

P.O. Box 9532
Allen, TX 75013
Toll-free: 888-397-3742

4. Further Information

You may obtain additional information about preventing identity theft by contacting the Federal Trade Commission or the Maryland Attorney General's Office, as follows:

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
Toll-Free: 1-877-438-4338
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Office of the Attorney General

200 St. Paul Place
Baltimore, MD 21202
Toll-Free: 1-888-743-0023
TDD: (410) 576-6372
<http://www.oag.state.md.us/>