

**Dominic A. Paluzzi**  
Direct Dial: 248.220.1356  
dpaluzzi@mcdonaldhopkins.com

RECEIVED  
OFF OF THE ATTY GENERAL

2016 JUL -8 P 4:07

McDonald Hopkins PLC  
39533 Woodward Avenue  
Suite 318  
Bloomfield Hills, MI 48304  
P 1.248.646.5070  
F 1.248.646.5075

June 23, 2016

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

**Re: Washington County Housing and Redevelopment Authority – Incident Notification**

Dear Sir or Madam:

McDonald Hopkins PLC represents Washington County Housing and Redevelopment Authority (“WCHRA”). I write to provide notification concerning a privacy incident that may affect the security of personal information of four (4) Maryland residents. WCHRA’s investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, WCHRA does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On March 14, 2016, WCHRA discovered that on that same day, as a result of a sophisticated network intrusion, an unauthorized third party gained access to one of its servers. Upon learning of the issue, WCHRA’s incident response team promptly launched an investigation and notified local law enforcement. As part of its investigation, WCHRA has been working very closely with one of the nation’s leading cybersecurity firms that regularly investigates and analyzes these types of incidents. Their investigation and remediation efforts are now completed, and WCHRA has removed the infection from its system. WCHRA also immediately changed passwords and took other steps to enhance the security of our network.

Based on a comprehensive forensic investigation and document review, which was concluded on June 8, 2016, WCHRA cannot conclusively determine whether the unauthorized party actually acquired or viewed any personal information. The unauthorized party, however, *may* have accessed some personal information within the infected server, including residents’ full names, Social Security numbers, and some driver’s license numbers.

Office of the Maryland Attorney General

June 23, 2016

Page 2

To date, WCHRA is not aware of any reports of identity fraud or improper use of information as a direct result of this incident. Nevertheless, we wanted to make you (and the affected residents) aware of the incident and explain the steps WCHRA is taking to safeguard the residents against identity fraud. WCHRA provided the Maryland residents with written notice of this incident commencing on June 23, 2016, in substantially the same form as the letter attached hereto. WCHRA has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. WCHRA is also offering the residents a complimentary one-year membership with a credit monitoring and identity theft restoration service and is providing dedicated call center support to answer questions. WCHRA has advised the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents have also been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

WCHRA is committed to maintaining the privacy of personal information and has taken many precautions to safeguard it. WCHRA is taking proactive steps to strengthen its IT systems moving forward to help prevent similar issues in the future.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or [dpaluzzi@mcdonaldhopkins.com](mailto:dpaluzzi@mcdonaldhopkins.com).

Sincerely,



Dominic A. Paluzzi

DAP/kjb

Encl.



Washington County  
Housing and Redevelopment Authority

Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

**IMPORTANT INFORMATION  
PLEASE READ CAREFULLY**

<<FirstName>><<LastName>>  
<<Address1>>  
<<Address2>>  
<<City, State ZIP>>

<<Date>>

Dear <<Name>>,

The privacy of your personal information is of the utmost importance to Washington County Housing and Redevelopment Authority (WCHRA). I am writing with important information about a recent incident involving the security of some of the personal information that we maintain. We want to provide you with information regarding the incident and explain the services we are making available to help safeguard you against identity fraud. We also are providing additional steps you can take to help protect your information.

On March 14, 2016, we discovered that on that same day, as a result of a sophisticated network intrusion, an unauthorized third party gained access to one of our servers. Upon learning of the issue, our incident response team promptly launched an investigation and notified local law enforcement. As part of our investigation, we have been working very closely with one of the nation's leading cybersecurity firms that regularly investigates and analyzes these types of incidents. Their investigation and remediation efforts are now completed, and we have removed the infection from our system. WCHRA also immediately changed passwords and took other steps to enhance the security of our network.

We have devoted considerable time and effort to determine what exact information may have been contained in the affected server and, as such, may be at risk of disclosure. However, based on our comprehensive forensic investigation and document review, which was concluded on June 8, 2016, we cannot conclusively determine whether the unauthorized party actually acquired or viewed any of your personal information. Because we value our relationship with you, we wanted to make you aware of this incident because the unauthorized party *may* have accessed some of your personal information within the infected server, including your full name and < Alt Address (Social Security number; driver's license number; bank account information)>.

**To date, we are not aware of any reports of identity fraud or improper use of information as a direct result of this incident.**

However, to protect you from potential misuse of your information, WCHRA is providing you with one year of free credit monitoring and identity theft protection services. Enclosed in this letter, you will find information on enrolling in a 12-month membership of Experian's ProtectMyID® Alert, a credit monitoring and identity theft protection service, along with other precautionary measures you can take to protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

Please accept my sincere apologies, on behalf of WCHRA, that this incident occurred – we deeply regret any inconvenience or concern this issue may cause you. Safeguarding the privacy and security of your personal information is a top priority, and we are taking proactive steps to strengthen our IT systems moving forward to help prevent similar issues in the future.

**If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at (888) 221-9891.** This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8 a.m. to 8 p.m. CST.

Sincerely,

A handwritten signature in black ink, appearing to read "Barbara Dacy". The signature is fluid and cursive, with the first name being more prominent.

Barbara Dacy  
Executive Director  
Washington County Housing and Redevelopment Authority

– OTHER IMPORTANT INFORMATION –

**1. Enrolling in Complimentary 12-Month Credit Monitoring.**

Protecting your personal information is important to Washington County Housing and Redevelopment Authority. In response to this security incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

***Activate Experian's® ProtectMyID Now in Three Easy Steps:***

1. ENSURE that you enroll by <Enrollment Date>.
2. VISIT the ProtectMyID Web Site to enroll: [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem)
3. PROVIDE your 9-character Activation Code: <Enrollment Code>

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide Engagement # <Engagement Number>.

***Additional Details Regarding Your 12-Month ProtectMyID Membership:***

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after an incident. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance:** Immediately covers certain costs including lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.)

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902.

**2. Placing a Fraud Alert.**

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
[www.equifax.com](http://www.equifax.com)  
1-800-525-6285

**Experian**  
P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

**TransUnion**  
P.O. Box 2000  
Chester, PA 19022  
[www.transunion.com](http://www.transunion.com)  
1-800-680-7289

### **3. Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

#### **Equifax Security Freeze**

PO Box 105788  
Atlanta, GA 30348  
<https://www.freeze.equifax.com>  
1-800-685-1111

#### **Experian Security Freeze**

PO Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
1-888-397-3742

#### **TransUnion Security Freeze**

P.O. Box 2000  
Chester, PA 19022  
<http://www.transunion.com/securityfreeze>  
1-800-680-7289

### **4. Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **[www.annualcreditreport.com](http://www.annualcreditreport.com)**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

### **5. Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If you live in **Iowa**, you may also report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General:

Office of the Iowa Attorney General  
Consumer Protection Division  
1305 East Walnut Street  
Des Moines, IA 50319  
(515) 281-5164  
1-888-777-4590  
Fax: (515) 281-6771  
[www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)

If you live in **Maryland**, in addition to the FTC, the Maryland Office of the Attorney General can also be contacted to obtain information on the steps you can take to avoid identity theft:

Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

If you live in *North Carolina*, in addition to the FTC, the North Carolina Office of the Attorney General can also be contacted to obtain information on the steps you can take to prevent identity theft:

North Carolina Department of Justice  
Office of the Attorney General  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-566-7226  
www.ncdoj.com

In addition, for federal public housing participants, the Deputy Assistant Secretary of Public Affairs for the U.S. Department of Housing and Urban Development (HUD) may be contacted for more information:

Cameron French  
Deputy Assistant Secretary of Public Affairs  
HUD  
451 7th Street S.W.  
Washington, DC 20410  
(202) 708-0980 ext. 5495

**6. Reporting Identity Fraud to the IRS.**

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- Contact your tax preparer, if you have one.
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police department.

Additional information regarding preventing tax related identity theft can be found at <http://www.irs.gov/uac/Identity-Protection>.