

RECEIVED
OFF OF THE ATTORNEY GENERAL

2016 MAY 31 P 6:28

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

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

May 11, 2016

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

Re: Abernathy & Company – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Abernathy & Company (“Abernathy”). I write to provide notification concerning an incident that may affect the security of personal information of two (2) Maryland residents. Abernathy’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, Abernathy does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Abernathy recently noticed some unusual activity on its computer system. Upon learning of the issue, Abernathy immediately commenced an investigation of the incident, including engaging external cybersecurity professionals, and retained an independent computer forensic firm to determine if any information was at risk. On April 12, 2016 Abernathy received notification that the forensic investigation concluded that an unauthorized third-party had accessed the server and obtained certain client information in a file.

Abernathy devoted considerable time and effort to determine what exact information may have been contained in the affected files and, as such, at risk of disclosure. Abernathy has confirmed that the compromised file contained 2014 tax returns, which included full names, addresses, dates of birth, and Social Security numbers, and may have included bank account numbers, to the extent it was provided for an electronic payment or refund.

Abernathy wanted to make you (and the affected residents) aware of the incident and explain the steps Abernathy is taking to help safeguard the residents against identity fraud. Abernathy is providing the Maryland residents with written notice of this incident commencing on May 12, 2016, in substantially the same form as the letter attached hereto. Abernathy is offering the residents a complimentary membership with a credit monitoring and identity theft protection service and is providing dedicated call center support to answer questions. Abernathy will advise the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Abernathy will advise the residents about the process for placing

Office of the Maryland Attorney General
May 11, 2016
Page 2

a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents also will be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Abernathy takes its obligation to help protect personal information very seriously. Abernathy is continually evaluating and modifying its practices to enhance the security and privacy of personal information.

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

Sincerely,



Dominic A. Paluzzi

Encl.

**ABERNATHY & COMPANY
CERTIFIED PUBLIC ACCOUNTANTS**



**IMPORTANT INFORMATION
PLEASE READ CAREFULLY**



<<Date>>

Dear 

The privacy of your personal information is of utmost importance to Abernathy & Company. We are writing to you with important information about a recent incident which may involve the security of some of your personal information that was supplied to us. We wanted to provide you with information regarding the incident, explain the services we are making available to help safeguard you against identity fraud, and provide steps you can take to help protect your information.

At the time of the incident we had significant measures in place to help protect your information, including: all applications are password protected which meet or exceed the industry accepted criteria for secure passwords, we utilize an enhanced commercial grade firewall, anti-virus and web protection programs are on all servers and workstations, updates are installed in a timely manner, and all stations are logged off or locked when not in use. However, we recently noticed some unusual activity on our computer system. We immediately commenced an investigation of the incident, including engaging external cybersecurity professionals and we retained an independent computer forensic firm to determine if any information was at risk. On April 12, 2016 the forensic investigation concluded that an unauthorized third-party had accessed the server and obtained certain client information in a file.

Since completing the forensic investigation, we have devoted considerable time and effort to determine what exact information may have been contained in the affected file and, as such, is at risk of disclosure. We can confirm that the compromised file contained your 2014 tax return, which included your full name, address, date of birth, and Social Security number, and may have included your bank account number, to the extent it was provided for an electronic payment or refund.

To date, we are not aware of any reports of identity fraud, theft, or other harmful activity related to the access of this file. Due to the complexity of the intrusion, we cannot conclusively determine whether the unauthorized user actually accessed any of your personal information. However, out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well.

Enclosed you will find information on enrolling in MyIDCare – identity theft protection services through ID Experts®, the data breach and recovery services expert, at no cost to you. ID Experts fully managed recovery services will include: 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials and complete access to their fraud resolution representatives. With this protection, ID Experts will help you resolve issues if your identity is compromised. We have also provided you with other precautionary measures you can take to help 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. Since your banking information may have been involved in this incident, we advise you to call your banking institution to determine if you should change your bank account number.

Please accept our sincere apologies that this incident occurred. We are committed to maintaining the privacy of our clients' information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of our clients' information.

If you have any further questions regarding this incident, please call us at [REDACTED] during regular business hours.

Sincerely,

[REDACTED]

Abernathy & Company

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Protecting your personal information is important to Abernathy. In response to this incident and as a precautionary measure, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare for a one year period at no cost to you. With this protection, ID Experts will help you resolve issues if your identity is compromised. We strongly encourage you to register for this free identity theft protection service.

To enroll please visit [REDACTED] or call [REDACTED]. You need to use the following Membership Code when enrolling: [REDACTED]

Your 12 month MyIDCare membership will include the following:

Complete Credit Monitoring and Recovery Services

- **Single Bureau Credit Monitoring** - Monitors any changes reported by Experian credit bureau to your credit report.
- **Access to the ID Experts Team** - Access to an online resource center for up-to-date information on new identity theft scams, tips for protection, legislative updates and other topics associated with maintaining the health of your identity.
- Should you believe that you are a victim of identity theft, ID Experts will work with you to assess, stop, and reverse identity theft issues.
- In the event of a confirmed identity theft, you may be eligible for reimbursement of up to \$1,000,000 for expenses related to that theft.

Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive ID Experts' Member Website where you will find other valuable educational information. The Membership Code expires on August 6, 2016.

Activate the credit monitoring provided as part of your membership with ID Experts. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. Note: You must have **established credit and access to a computer and the internet to use this service. If you need assistance, ID Experts will be able to assist you.**

If you discover any suspicious items and have enrolled with ID Experts, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with ID Experts, you will be contacted by a member of the Recovery Department who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Experts Recovery Advocate who will work on your behalf to identify, stop and reverse the damage quickly.

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
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
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**. 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, 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.

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

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:

- 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 to report the situation.

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