McDonald Hopkins
A business advisory and advocacy law firm®

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

RECEIVED
OFF OF THE ATTY GENERAL
2016 JUN 27 P 6:45

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

June 6, 2016

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

Re: Flynn & Company, Inc. Certified Public Accountants – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Flynn & Company, Inc. Certified Public Accountants ("Flynn"). I write to provide notification concerning a privacy incident that may affect the security of personal information of three (3) Maryland residents. Flynn'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, Flynn does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

After receiving notice that its attempts to file some of their clients' tax returns had been rejected, Flynn commenced a prompt investigation. As part of its investigation, Flynn retained a national third-party computer forensic firm to analyze its internal systems, which are outsourced and managed by their third-party IT provider, for any unusual or unauthorized activity.

On May 26, 2016, the forensic investigation concluded that, beginning on March 1, 2016, a foreign third-party had gained unauthorized access to Flynn's systems and could have viewed or acquired certain files containing client information. After discovering the issue, Flynn promptly changed all passwords to its internal system and implemented the use of two-factor authentication to access its third-party IT provider's system.

Since completing the forensic investigation, Flynn has devoted considerable time, effort and cost to determine what exact information may have been accessed and/or acquired by the unauthorized party within its system and, as such, at risk of disclosure. Flynn can confirm that the files that may have been accessed contained the residents' full names and Social Security numbers. To the extent the residents supplied Flynn with their driver's license and/or bank account numbers (routing and checking) for refund or payment purposes, then that information may have been accessed as well.

Due to the complexity of the intrusion, we cannot conclusively determine whether the unauthorized user actually acquired or viewed any personal information. Nevertheless, we wanted to make you (and the affected residents) aware of the incident and explain the steps Flynn is taking to safeguard the residents against identity fraud. Flynn provided the Maryland residents with written notice of this incident commencing on June 6, 2016, in substantially the same form as the letter attached hereto. Flynn has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Flynn 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. Flynn 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.

Flynn is committed to maintaining the privacy of personal information and has taken many precautions to safeguard it. As part of its investigation with its national computer forensic specialist, Flynn has audited its outsourced third-party IT provider to minimize the risk of a similar situation in the future.

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

Sincerely,

Dominic A. Paluzzi

DAP/kjb
Encl.

Flynn & Company
CPAs & Business Consultants
7800 E. Kemper Road • Suite 150
Cincinnati, OH 45249

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

<<mail id>>
<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name 1>>,

The privacy of your personal information is of utmost importance to Flynn & Company, Inc. Certified Public Accountants (Flynn). We are writing to you with important information about a recent incident that may involve some of your personal information that was supplied to us. While cybersecurity threats continue to impact all of us, we are taking ever-increasing measures to protect your information.

After receiving notice that our attempts to file some of our clients' tax returns had been rejected, we commenced a prompt investigation. As part of our investigation, we retained a national third-party computer forensic firm to analyze our internal systems, which are outsourced and managed by our third-party IT provider, for any unusual or unauthorized activity.

On May 26, 2016, the forensic investigation concluded that, beginning on March 1, 2016, a foreign third-party had gained unauthorized access to our systems, which are outsourced and managed by our third-party IT provider, and could have viewed or acquired certain files containing client information. After discovering the issue, we promptly changed all passwords to our internal system and implemented the use of two-factor authentication to access our third-party IT provider's system.

Since completing the forensic investigation, we have devoted considerable time, effort and cost to determine what exact information may have been accessed and/or acquired by the unauthorized party within our system and, as such, at risk of disclosure. We can confirm that the files that may have been accessed contained your full name and Social Security number. To the extent you supplied us with your driver's license and/or bank account numbers (routing and checking) for refund or payment purposes, then that information may have been accessed as well.

Due to the complexity of the intrusion, we cannot conclusively determine whether the unauthorized user actually acquired or viewed any of your personal information. Out of 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 a 12-month membership of Experian's ProtectMyID® Alert, that we are providing at no cost to you, 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 know that we are committed to maintaining the privacy of our clients' information. As part of our investigation with our national computer forensic specialist, they have audited our outsourced third-party IT provider to minimize the risk of a similar situation in the future.

Please accept our sincere apologies that this incident occurred. **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) 293-0018.** 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, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Richard T. Flynn, CPA
Flynn & Company, Inc. Certified Public Accountants

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Protecting your personal information is important to Flynn & Company, Inc. Certified Public Accountants. 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 **September 7, 2016**.
2. VISIT the ProtectMyID Web Site to enroll: **www.protectmyid.com/redeem**
3. PROVIDE your 9-character Activation Code: **<<Account Code>>**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide Engagement # PC101831.

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 877-288-8057.

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	**Experian**	**TransUnion**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	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.

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

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

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.