

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

April 3, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

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

Re: Fitness Cubed – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Healthii Holdings, Inc., I am writing to provide notification of an incident at Fitness Cubed doing business as Cubii, a subsidiary company of Healthii Holdings, Inc., that may affect the security of personal information of approximately three (3) Maryland residents. Cubii's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Cubii does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On March 24, 2023, Cubii received information indicating that some employees received notice from the Internal Revenue Service that an unauthorized party filed tax returns in their name. Upon learning of the issue, Cubii commenced a prompt and thorough investigation. Cubii learned that on January 25, 2023, an unauthorized actor obtained access to certain individuals' W2 statements as a result of a phishing incident. Upon learning of this issue, Cubii immediately commenced an internal investigation and promptly notified potentially affected individuals. Cubii also notified the IRS, FBI, and state and local law enforcement.

Cubii wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Cubii is providing the affected residents with written notification of this incident commencing on or about April 3, 2023 in substantially the same form as the letter attached hereto. Cubii is offering residents complimentary one-year membership with a credit monitoring service. Cubii will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Cubii will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact

April 3, 2023

Page 2

information for the consumer reporting agencies, the Maryland Attorney General, and the Federal Trade Commission.

At Cubii, protecting the privacy of personal information is a top priority. Cubii is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Cubii continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,



James J. Giszczak

Encl.



**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

April 3, 2023

Dear [REDACTED]

The privacy and security of the personal information entrusted to us is of the utmost importance to Cubii. We are writing to provide you with additional information, as indicated in our March 24th email, regarding a recent incident which involves the security of some of your personal information that was supplied to us. We want to provide you with information regarding the incident and explain the services we are making available to help safeguard against identity fraud. We also are providing additional steps you can take to further protect your information.

What Happened?

On March 24, 2023 we received information indicating that some of our employees received notice from the Internal Revenue Service that an unauthorized party filed tax returns in their name. Upon learning of the issue, we commenced a prompt and thorough investigation. We learned that on January 25, 2023, an employee received a phishing email, purporting to be a leadership team member, requesting W2 statements. The employee subsequently responded, providing a number of 2022 W2 statements to the unauthorized individual.

What Information Was Involved?

The impacted information includes that which is contained on your W2: your name, address, Social Security number, and earnings information.

What We Are Doing.

We immediately conducted a thorough investigation and notified the IRS, FBI, and state and local law enforcement. The employee responsible is no longer employed at Cubii. Out of an abundance of caution, we want to make you aware of the incident and provide you with one year of complimentary credit monitoring services.

What You Can Do.

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

If your tax return was rejected **or** you received a tax notice from a government agency (such as a notice from the IRS indicating someone was otherwise using your Social Security number), we recommend that you follow the below guidance:

- Respond immediately to any IRS notice you receive, and call the number provided and/or follow the instructions contained in the notice;
- 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>).
- You may choose to opt-in to the IRS Identity Protection (IP) PIN Program. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. To opt-in, you should use the online “Get an IP PIN” tool (which can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>). If you don’t already have an account on IRS.gov, you must register to validate your identity. An IP PIN is valid for one calendar year. You must obtain a new IP PIN each year. The IP PIN tool is generally unavailable mid-November through mid-January each year.
- If you are filing Form 14039, you should also check with your local state tax agency to see if there are any additional steps to take at the state level for reporting tax-related identity theft;
 - A complete listing of each state tax agency’s website can be found at: <https://www.taxadmin.org/state-tax-agencies>.
- Review guidance from the IRS about tax-related identity theft at: <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft> (*Taxpayer Guide to Identity Theft*) and <https://www.irs.gov/pub/irs-pdf/p5027.pdf> (*IRS Publication 5027, Identity Theft Information for Taxpayers*); and/or
- Call or visit your local law enforcement agency and file a police report.

Keep in mind that if you have an open identity theft case that is being worked on by the IRS, you need to continue to file your tax returns while the investigation is ongoing. Additional information regarding preventing tax related identity theft can be found at: <http://www.irs.gov/uac/Identity-Protection>.

In addition to the above, we also recommend that you take additional steps with agencies outside of the IRS, and report incidents of identity theft to the Federal Trade Commission and contact the fraud departments of the three major credit bureaus. More information, including contact information, for these agencies can be found in the attachment.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please contact Danny Baumwald at danny@mycubii.com or (410) 340 - 4500, Monday through Friday during normal business hours.

Sincerely,

Danny Baumwald
Cubii

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12 months Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by 7/31/2023** at no later than 5:59pm CT (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bplus>
- Provide your **activation code**: [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by 7/31/2023. Be prepared to provide engagement number B088975 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

2. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 1-year “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 other credit bureaus.

Equifax

P.O. Box 105788
Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013

<https://www.experian.com/fraud/center.html>

(888) 397-3742

TransUnion LLC

P.O. Box 6790
Fullerton, PA 92834-6790

<https://www.transunion.com/fraud-alerts>

(800) 680-7289

3. **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, at no charge. 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 or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(800) 349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016

<http://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

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. Reporting Identity Fraud to the IRS.

If you believe 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 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, 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 or law enforcement department.

You may also request an Identity Protection PIN from the IRS. The Identity Protection PIN is a six-digit number the IRS assigns to an individual to help prevent misuse of their Social Security number or Individual Taxpayer Identification Number on federal tax returns. The IRS may automatically assign an Identity Protection PIN if you are a confirmed victim of tax-related identity theft. Otherwise, you can request an Identity Protection PIN at: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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

6. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount. The Social Security Administration has published Identity Theft and Your Social Security Number at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

7. 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 this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.