

Christine Czuprynski
Direct Dial: 248.220.1360
E-mail: cczuprynski@mcdonaldhopkins.com

June 8, 2022

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

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

Re: Long Fence Company, Inc. – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents Long Fence Company, Inc. I am writing to provide notification of an incident at Long Fence that may affect the security of personal information of 3,927 Maryland residents. Long Fence's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any.

On February 27, 2022, Long Fence detected that a ransomware infection began encrypting files stored on their network. Upon learning of this issue, Long Fence contained the threat by disabling all unauthorized access to the network, restored all encrypted data, and immediately commenced a prompt and thorough investigation. As part of the investigation, Long Fence has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Though the investigation is ongoing, Long Fence determined on May 10, 2022 that the perpetrator may have removed certain files and folders from the network. The impacted files contain personal information belonging to Long Fence employees and staff.

Long Fence has no indication that any information has been misused. Nevertheless, out of an abundance of caution, Long Fence is providing notice to the affected residents commencing on June 9, 2022 in substantially the same form as the document attached hereto. Residents whose Social Security numbers are impacted will receive complimentary credit monitoring services. Additionally, Long Fence will advise the affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Long Fence will further 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 provided with the contact information for the consumer reporting agencies, the Maryland Attorney General, and the Federal Trade Commission.

June 8, 2022

Page 2

Protecting the privacy of personal information is a top priority for Long Fence Company, Inc. Long Fence remains fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. Long Fence continually evaluates and modifies practices to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

A handwritten signature in black ink, appearing to read "Christine Czuprynski", with a stylized, flowing script.

Christine N. Czuprynski

Encl.

LONG FENCE®

Return Mail Processed By:
IDX
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:

1-833-909-4274

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: [REDACTED]

June 9, 2022

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to Long Fence Company, Inc. ("Long Fence"). We are writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident, inform you about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On February 27, 2022, Long Fence detected that a ransomware infection began encrypting files stored on our network.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling all unauthorized access to our network, restored all encrypted data, and immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Though the investigation is ongoing, Long Fence determined on May 10, 2022 that the perpetrator may have removed certain files and folders from the network. The impacted files contain personal information belonging to Long Fence employees and staff.

What Information Was Involved.

The impacted files contained some of your personal information, specifically your address, [REDACTED].

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership in identity theft protection services through IDX, the data breach and recovery services provider. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on identity theft prevention and IDX identity protection services 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/or security freeze on your credit files, and/or 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.

For More Information.

Please accept our apologies that this incident occurred. We remain fully 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 to enhance the security and privacy of your personal information.

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 [REDACTED]. 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 am – 9 pm Eastern Time.

Sincerely,

Long Fence Company, Inc.
8545 Edgeworth Drive
Capitol Heights, MD 20743

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Please note that the enrollment deadline is September 9, 2022.

Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one (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 others.

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, CA 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 contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

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

[freeze/](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

<https://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 reporting 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. 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 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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

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: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

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.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.