



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 5, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Franklin Park Conservatory and Botanical Gardens (“The Conservatory”) located at 1777 E Broad Street, Columbus, OH 43203, and are writing to notify your office of an incident that may affect the security of some personal information relating to six (6) Maryland residents. By providing this notice, The Conservatory does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 21, 2021, The Conservatory detected a cyber event impacting its internal systems. The Conservatory immediately secured its network and launched an investigation with the assistance of third-party computer specialists to determine the nature and scope of the incident. The investigation determined that certain files on The Conservatory’s systems may have been subject to unauthorized access between July 16, 2021 and July 21, 2021. During this time period, the unauthorized actor viewed and potentially stole certain files. The Conservatory then began a review of the affected files to determine what, if any, sensitive information was contained therein. The review was completed on November 1, 2021, after which point The Conservatory worked to locate address information for the impacted individuals in order to effectuate notice.

The information that could have been subject to unauthorized access includes name, address, and Social Security number.

Notice to Maryland Residents

On January 4, 2022, The Conservatory provided written notice of this incident to all affected individuals, which includes six (6) Maryland residents. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, The Conservatory moved quickly to investigate and respond to the incident, assess the security of The Conservatory systems, and notify potentially affected individuals. The Conservatory is also working to implement additional safeguards and training to its employees. The Conservatory is providing access to credit monitoring services for one (1) year, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, The Conservatory is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. The Conservatory is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM/ara
Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>,

Franklin Park Conservatory and Botanical Gardens ("The Conservatory") is writing to make you aware of an incident that may have affected the security of some of your information. While we are not aware of any actual or attempted misuse of your information, we are providing you with an overview of the incident, our ongoing response, and resources available to you right now to help protect your information, should you feel it is appropriate to do so.

What Happened?

On July 21, 2021, The Conservatory detected a cyber event impacting our internal systems. We immediately secured our network and launched an investigation with the assistance of third-party computer specialists to determine the nature and scope of the incident. The investigation determined that certain files on The Conservatory's systems may have been subject to unauthorized access between July 16, 2021 and July 21, 2021. During this time period, the unauthorized actor viewed and potentially stole certain files. We then began a review of the affected files to determine what, if any, sensitive information was contained therein. On November 1, 2021, our review was completed and we determined that the files contained certain information related to you.

What Information Was Involved?

The Conservatory determined that the following information related to you was present in the affected files at the time of the incident: your name and <<data elements>>.

What We Are Doing.

We take this incident and the security of information within our care seriously. Upon discovery of this incident, we launched an investigation with the assistance of third-party forensic investigators to determine the full nature and scope of this incident. As part of our ongoing commitment to the privacy of information in our care, we reviewed our existing policies and procedures and implemented additional safeguards to further secure the information in our systems as appropriate.

As an added precaution, we are also offering <<12/24>> months of complimentary access to credit monitoring services through Equifax. Individuals who wish to receive these services must enroll by following the enrollment instructions found in the enclosed *Steps You Can Take to Help Protect Personal Information*.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months.

For More Information.

We understand that you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered promptly, please contact our dedicated and toll free response line at 855-604-1691, Monday through Friday 9:00 am to 9:00pm Eastern Time.

Sincerely,

A handwritten signature in black ink, appearing to read 'B. Harkey', with a large, stylized '3' or 'B' at the beginning and a horizontal line extending to the right.

Bruce A. Harkey
President and CEO
Franklin Park Conservatory and Botanical Gardens

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring



Enter your Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourage potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate.

Enter your unique Activation Code of <<ACTIVATION CODE>> then click “Submit” and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click “Continue”.
If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click ‘Sign Me Up’ to finish enrolling.
You’re done!
The confirmation page shows your completed enrollment.
Click “View My Product” to access the product features.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

¹ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded.

² The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁴ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and www.oag.state.md.us. Franklin Park Conservatory and Botanical Gardens is located at 1777 E Broad Street, Columbus, OH 43203.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are Rhode Island residents impacted by this incident.