

India Vincent
ivincent@burr.com
Direct Dial: (205) 458-5284
Direct Fax: (205) 244-5714

Burr & Forman LLP
171 17th Street, NW
Suite 1100
Atlanta, GA 30363

Office (404) 815-3000
Fax (404) 817-3244

BURR.COM

July 20, 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: Data Breach Notification Under Maryland Code § 14-3504

Dear Office Maryland Attorney:

On behalf of our client, Bright Future Electric, LLC (“**Bright Future**”), we are providing this Notice of Security Breach in accordance with the Maryland Personal Information Protection Act (Md. Code Ann. Comm. Law § 14-3504).

The Incident

On June 24, 2023, Bright Future's computer systems were attacked by a criminal actor, and the attack resulted in encryption of several of Bright Future's computer servers, including a file server. The attack was quickly contained, and Bright Future worked with IT service providers, forensic consultants, and legal counsel to investigate the incident and repair its systems. Bright Future also notified the FBI of the attack and has cooperated with the FBI's investigation.

The investigation has revealed that certain files from Bright Future's file servers were copied by the attackers. At this time, Bright Future has not been able to verify the specific files that were viewed or copied, nor is Bright Future able to confirm the content of those files at this time. The investigation is continuing.

Data Involved

While the company's primary database for employee information was not compromised, Bright Future currently believes the copied files may have contained reports that could have included personal information of at least some of Bright Future's employees. Bright Future has determined that the data in the files that may have been accessed could have included individuals' names, information used to verify employment eligibility, payroll information, identifiers such as social security numbers, driver's license numbers, state ID numbers, military ID numbers, and passport numbers, financial account numbers that we have on file for direct deposit purposes (but not any codes or passwords that would allow access to the financial accounts), information about the

July 20, 2023

Page 2

individual's physical or mental health, but only if the individual provided information regarding their physical or mental health for purposes of receiving accommodations in their job function, and health insurance policy numbers.

Who Is Being Notified

The company currently believes the files may have contained reports that included personal information of at least some of Bright Future's current and former employees. Out of an abundance of caution, Bright Future made the decision to notify all current and former employees of the incident. There are two Maryland residents in the population of Bright Future's current and former employees.

The Notice

The attached notice will be emailed to those two individuals on Friday, July 21, 2023 and a hard copy mailed via USPS the week of July 24, 2023.

Assistance to Notice Recipients

Bright Future is offering Norton LifeLock's Defender Choice protection to each current and former employee, free of charge, for one year. Information on how to sign-up for this service is included in the attached notice letter.

Steps the Company Is Taking

Bright Future continues to work with forensic experts and its legal counsel to understand the cause and scope of the incident and to fully restore its systems. In addition, concurrently with its restoration efforts, Bright Future has taken several steps to strengthen its security posture. In particular, Bright Future has moved additional data to the Cloud, has implemented stronger password requirements, and is requiring two-factor authentication for all system access. Bright Future will continue to monitor its systems for opportunities to incorporate additional safeguards to protect from future attacks.

Additional Information

For additional information regarding the incident, please contact:

Name:	India Vincent
Title:	Legal Counsel to Bright Future Electric, LLC
Company:	Burr & Forman, LLP
Address:	420 North 20th Street, Suite 3400 Birmingham, AL 35223
Telephone Number:	205-458-5284
Email Address:	ivincent@burr.com

The company's address is 3420 Richard Arrington Jr. Blvd N., Birmingham, AL 35234, and their website is brightfutureelectric.com.

Sincerely,

/s/ *India E. Vincent*

India E. Vincent

Attorney, Burr & Forman LLP

Exhibit A

Notice Letter to Two Maryland Residents

(see attached)



3420 Richard Arrington Jr Blvd N
Birmingham, AL 35234

July 21, 2023

NOTICE OF DATA SECURITY INCIDENT

Bright Future values each employee and your contributions to our organization. We understand the importance of maintaining the privacy of your information, which is why, out of an abundance of caution, we are writing to provide you with additional information about the recent cybersecurity attack that may affect the security of some of your personal information. While we currently have no evidence of actual misuse of your information, we want to provide you with additional information about the incident, our response to it, and information how you may better protect your personal information.

WHAT HAPPENED?

On Saturday, June 24, 2023, we became aware of a criminal attack on our computer systems. We acted immediately to contain the attack, but several of our computer servers were encrypted as a result of the attack. We contained the attack and began an investigation, while simultaneously working to get the encrypted servers back up and running. During the course of the investigation, we learned that the criminal actors made copies of some of the files stored on the encrypted computer servers. We do not yet know which of the files were viewed or copied or the content of those files. While we cannot confirm that your personal information was viewed or copied by the unauthorized actor, we cannot rule out that possibility at this time. The investigation is continuing, and we will let you know if there is new information that impacts your personal information.

WHAT INFORMATION WAS INVOLVED?

All data stored in our accounting and human resource system is encrypted by the system when it is stored. That data was not accessed or taken by the criminal actor. However, there were certain reports and documents stored on a protected drive on our main file server that contained reports that included some personal information.

The information in the compromised data may have included

- Names;
- Information used to verify your employment eligibility;
- Payroll information;
- Identifiers such as social security numbers, driver's license numbers, state ID numbers, military ID numbers, and passport numbers;
- Financial account numbers that we have on file for direct deposit purposes (note that we do not collect or store any codes or passwords that would allow access to your financial accounts, only your account number);
- If you have provided it to us for purposes of receiving accommodations in your job function, information regarding your physical or mental health; and
- Health insurance policy numbers.

Because we do not yet know which report files were copied or whose personal information was included in the reports, nor do we know what data about each individual was included in those reports, we are notifying all current and employees. As we learn more we will notify you if there are any developments that have bearing on your personal information.

WHAT WE HAVE DONE

Information, privacy and security are among our highest priorities. Immediately upon learning of this attack, we engaged our IT service providers and a security consultant for assistance containing and remediating the incident. Out of an abundance of caution, we also promptly disabled access to the affected systems. We also engaged a forensic team to investigate the incident. In addition, we engaged legal counsel and reported this incident to law enforcement. We continue to cooperate with law enforcement in their investigation.

WHAT WE ARE DOING

We value your privacy and deeply regret this occurred. At this time, we are continuing to thoroughly review the affected servers and files to ensure the integrity of the data. We are also continuing to work with the forensic team, law enforcement,

July 20, 2023

Page 5

and our legal counsel to investigate this incident. If we are able to determine with more certainty what data was in the files that were copied, we will provide a further update.

As we work to restore the system, we are taking several steps to strengthen our security posture. In particular, we are moving additional data to the Cloud, are implementing stronger password requirements, and are requiring two-factor authentication for all access to the Bright Future system. You may notice some changes in the way you access our systems as a result of these changes. We will continue to monitor our systems for opportunities to incorporate additional safeguards to protect from future attacks, because protecting the privacy and security of your information is always a high priority for Bright Future.

In addition, we have secured the services of Norton LifeLock Inc. to provide all current and former employees with a one-year subscription of identity theft and credit monitoring services, at no cost to you. Please review the enclosed Norton LifeLock Enrollment Information for additional detail including enrollment instructions.

WHAT YOU CAN DO

We encourage you remain extra vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained and report the incident to proper law enforcement authorities, including your local law enforcement, state attorney general, and the Federal Trade Commission (FTC).

We also encourage you to enroll with Norton LifeLock to receive the identity theft and credit monitoring services we are providing. Please note that you must enroll directly, as Bright Future is unable to enroll you directly. We strongly encourage you to sign up for this service at your earliest opportunity.

To file a complaint with the FTC, go to IdentityTheft.gov, call 877-ID-THEFT (877-438-4338), or mail your complaint to the FTC at 600 Pennsylvania Avenue, NW, Washington, DC 20580, using OMB CONTROL#: 3084-0169. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Please review the attachment, "Steps You Can Take to Further Protect Your Information."

FOR MORE INFORMATION

For further information and assistance about the incident or the types of personal information Bright Future maintains about you, please contact the Bright Future – Norton LifeLock Help Line at <<Insert Number>>, from 8 a.m. to 5 p.m. CST Monday through Friday. Representatives with the Bright Future –LifeLock Help Line can also provide you with the toll-free numbers and addresses for the major credit reporting agencies, which also appear in the attachment to this letter.

Sincerely,

[INSERT SIGNATURE]

[INSERT TITLE]

Please note that this is the same information you should have received by email. You only need to register for Norton LifeLock once.

Steps You Can Take to Further Protect Your Information

Complimentary Credit Monitoring and Identity Protection Services

Bright Future has retained Norton LifeLock, Inc. to provide one (1) Year of complimentary LifeLock Defender™ Choice identity theft protection.

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to <<Offer URL>>.
(do not attempt registration from a link presented by a search engine).
2. Below the three protection plan boxes, enter the **Promo Code:** <<Promo Code>> and click the “APPLY” button.
3. Your complimentary offer is presented. Click on the orange “**START YOUR MEMBERSHIP**” button.
4. A popup will appear to enter your **Member ID:** <<MEMBER ID>>. Once entered, click the “APPLY” button.
5. Once enrollment is completed, you will receive a confirmation email
(be sure to follow ALL directions in this email).

Alternatively, to activate your membership by phone, please call: <<Phone Number>> and select option 1.

**You have until <<INSERT DATE>>, 2023
to enroll in the Norton LifeLock Service.**

Once you have completed the LifeLock enrollment process, the service will be in effect. Your LifeLock Defender™ Choice membership includes:

- | | |
|---|---|
| ✓ Primary Identity Alert System [†] | ✓ 24/7 Live Member Support |
| ✓ Dark Web Monitoring | ✓ Norton™ Security Deluxe ² (90 Day Free Subscription) |
| ✓ Stolen Funds Reimbursement up to \$25,000 ⁺⁺⁺ | ✓ Personal Expense Compensation up to \$25,000 ⁺⁺⁺ |
| ✓ Coverage for Lawyers and Experts up to \$1 million ⁺⁺⁺ | ✓ U.S.-based Identity Restoration Team |
| ✓ Annual Single-Bureau Credit Reports & Credit Scores ^{1**} | ✓ Single-Bureau Credit Monitoring ^{1**} |
| ✓ Credit, Checking and Savings Account Activity Alerts ^{†**} | |

¹ If your plan includes credit reports, scores, and/or credit monitoring features (“Credit Features”), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment. No one can prevent all identity theft or cybercrime. [†] LifeLock does not monitor all transactions at all businesses.

² Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.

^{**} These features are not enabled upon enrollment. Member must take action to get their protection.

⁺⁺⁺ Reimbursement and Expense Compensation, each with limits of up to \$25,000 for Defender Choice. And up to \$1 million for coverage for lawyers and experts if needed, for all plans. Benefits provided by Master Policy issued by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554 Allen,
TX 75013
888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security Number;
- Date of Birth;
- If you have moved in the past 5 years, provide the addresses where you have lived over the past 5 years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 agencies listed above.

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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 North Carolina residents, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699- 9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1- 410-528-8662; or www.oag.state.md.us.

For New Mexico residents, individuals have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in the individual's credit file has been used against the individual, the right to know what is in an individual's credit file, the right to ask for an individual's credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to an individual's file is limited; an individual must give consent for credit reports to be provided to employers; an individual may limit "prescreened" offers of credit and insurance an individual would get based on information in a credit report; and an individual may seek damages from violator. An individual 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 individuals to review their 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 Rhode Island residents, The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; or 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 two (2) Rhode Island residents impacted by this incident.

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