McGuireWoods LLP
Gateway Plaza
800 East Canal Street
Richmond, VA 23219-3916
Phone: 804.775.1000
Fax: 804.775.1061
www.mcguirewoods.com

Janet Peyton
Direct: 804.775.1166

McGUIREWOODS

jpeyton@mcguirewoods.com
Fax: 804.698.2230

July 1, 2021

VIA FEDERAL EXPRESS
The Honorable John Formella
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Notice of Data Breach – Supplemental Information

Dear Attorney General Formella:

I am writing on behalf of Direct Energy LP and its affiliates First Choice Power, Inc. and Home Warranty of America, Inc. (collectively, "Direct Energy"), with a headquarters located at 12 Greenway Plaza #250, Houston, TX 77046, to provide supplemental notice to your office, with respect to our enclosed letter to former Attorney General Gordon MacDonald dated December 1, 2020. *See* **Exhibit A**. This notice is supplemental only with respect to the number of impacted individuals. All of the other information reported in our initial letter to your office remains the same.

In our December 1 letter, we provided details regarding the number of New Hampshire residents that had certain types of information involved in the incident. Since then, we have identified additional factors that increased these counts. Specifically, our further investigations revealed that, in total, the credit card details of an additional eight New Hampshire residents (for a total of 23) were involved in the incident and the bank account information of one additional New Hampshire resident (for a total of five) was involved. As we reported to former Attorney General MacDonald previously, the incident also involved a breach of account holders' usernames and passwords, and while this information is not subject to notification under N.H. Rev. Stat. § 359-C:20 (because it does not provide access to a financial account), Direct Energy did notify these customers as well. The number of New Hampshire residents in this category increased by 18 for a total of 1,163 New Hampshire residents.

There are several reasons why our further investigation revealed that the number of New Hampshire residents whose information was involved in the incident is greater than what we originally reported to former Attorney General MacDonald. First, we discovered that there were

some accounts *with multiple individuals'* names on a *single* account at a single address, and as such, they were initially counted as a single individual for purposes of the breach notifications. Our original count relied on the number of impacted accounts, which we now know sometimes included multiple individuals. As such, while the overall count of New Hampshire residents has increased, we confirm that, on December 2, 2020, we sent notices addressed to all of these individuals, but in the cases of multiple individuals listed on a single account (such as spouses or roommates) they received a single letter with both names, in the manner of the names as they appeared on the Direct Energy account. In any instances where a recipient of our notice letters called to redeem the credit monitoring services that Direct Energy offered in the letter and asked for an additional code for a second individual to whom the letter was directed, Direct Energy provided an additional code free of charge.

Additionally, after we sent our December 2 letters to the New Hampshire residents identified in the original incident and sent our original notification to your office, our further investigation revealed additional data that was involved in the breach. This resulted in our discovery of additional affected New Hampshire residents that were not accounted for in our December 1 letter to former Attorney General MacDonald. We sent notices to these residents on or before December 22, 2020.

Finally, upon receiving returned mail or non-deliverable notices from the earlier mailings, our subsequent research to locate updated addresses revealed that some of the impacted consumers had moved to different states, thereby impacting the total number of affected residents in some states. For accuracy, we waited to provide supplemental notices to all state Attorneys General until this research was completed this month. Fortunately, with respect to New Hampshire, this did not reveal any further changes in the number of impacted residents.

If you have questions about this incident, please feel free to contact me at the email or phone numbers listed above.

Sincerely,

Janet P. Peyton

Enclosure: Exhibit A: December 1, 2020 Letter to Attorney General MacDonald (w/enclosures)

cc: Valerie Daniel, Esq. Direct Energy (via email w/encl.)

EXHIBIT A

McGuireWoods LLP
Gateway Plaza
800 East Canal Street
Richmond, VA 23219-3916
Phone: 804.775.1000
Fax: 804.775.1061
www.mcguirewoods.com

Janet Peyton
Direct: 804.775.1166

McGUIREWOODS

jpeyton@mcguirewoods.com
Fax: 804.698.2230

December 1, 2020

VIA FEDERAL EXPRESS
The Honorable Gordon MacDonald
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Notice of Data Breach

Dear Attorney General MacDonald:

I am writing on behalf of Direct Energy LP and its affiliates First Choice Power, LLC and Home Warranty of America, Inc., (collectively, "Direct Energy") with a headquarters located at 12 E. Greenway Plaza #250, Houston, TX 77046, to provide a report of a recent data breach. Direct Energy is a retail provider of electricity and natural gas, as well as certain home warranty services. On November 3, 2020, Direct Energy was notified by one of its data analytics vendors, Kitewheel, LLC ("Kitewheel") that earlier that day Kitewheel was the subject of a "ransomware" attack on their systems. During the November 3 incident, unauthorized individuals accessed and extracted some of Kitewheel's client files, including files that contained personal information of Direct Energy's customers.

The personal information that was extracted from Kitewheel's systems included certain customers' user names and passwords for Direct Energy online accounts, customer payment card information, or in some cases, all of the foregoing. Based on the results of our forensic investigations, we believe that the group of impacted customers included 15 New Hampshire residents whose credit card information was involved in the incident, four New Hampshire residents whose bank account information was involved, and 1,141 New Hampshire residents whose usernames and passwords were involved. While we recognize that the username and password information is not deemed "personal information" subject to notification under N.H. Rev. Stat. § 359-C:20 (because it does not provide access to a financial account) Direct Energy is notifying its customers of the breach of their usernames and passwords out of an abundance of caution. Notices are being sent to the impacted customers on December 2, 2020.

Kitewheel contained the incident and immediately commenced an investigation, in cooperation with Direct Energy. Kitewheel also retained a forensic expert and notified the FBI of the incident. Direct Energy is also conducting its own investigation into the scope and extent of the compromised data. Further, Direct Energy instituted a mandatory password reset across all impacted customers, and (other than cooperation in connection with the investigation) has temporarily suspended all commercial activity with Kitewheel. With respect to payment card data, we have notified Visa, Mastercard, American Express and Discover and certain payment processor entities, so that they may take appropriate action to protect cardholders. In addition, Direct Energy is offering each impacted customer a complimentary two-year membership in Experian's® IdentityWorks^{SM}.

I have enclosed a copy of the form of notification letter that will be sent to affected individuals on December 2, 2020. As you will see, among other things, the letter describes various steps that affected individuals can take to protect themselves, provides contact information for consumer reporting agencies and relevant governmental agencies and provides information about enrolling in two years of credit monitoring services that will be provided to the individuals by Direct Energy at no cost. Also enclosed is an Appendix which will serve as a key for your reference to the "Extra" fields in the letter, which are variables depending on the particular personal information involved.

If you have questions about this incident, please feel free to contact me at the email or phone numbers listed above.

Sincerely,

Janet P. Peyton

Enclosure: Template Notification Letter

cc: Valerie Daniel, Esq. Direct Energy (via email, w/encl.)

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

December 2, 2020

G0132-L1A-0000001 T00001 P001 **********MIXED AADC 159
SAMPLE A SAMPLE - L01 A - DIRECT ENERGY
COMPANY
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

RE: Notice of Data Breach

Dear Sample A Sample:

I am writing to you on behalf of Direct Energy LP ("Direct Energy") with important information about a data security incident that occurred on November 3, 2020 at a vendor that provides data analytics services for us. [EXTRA1] takes the protection and proper use of your personal information very seriously. We are, therefore, contacting you to explain the incident and provide you information about security measures you can take to protect yourself and your personal information.

What Happened:
On November 3, 2020, we were notified of a data security incident that occurred at one of our data analytics vendors, which involved some of [EXTRA1]'s customer information. The incident involved a "ransomware" attack on the vendor's systems on November 3, 2020. On that date, it appears that unauthorized parties accessed and extracted some of the vendor's client files, including some files containing customer information of [EXTRA1]. In accordance with the standard recommendation of the FBI and financial regulators, the vendor did not pay the ransom, and immediately began working to contain the incident and terminate any unauthorized access. [EXTRA2] This notice was not delayed as the result of a law enforcement investigation.

What Information Was Involved:
This incident involved your [EXTRA3]. As a result, your personal information may have been exposed to others.

What We Are Doing:
We understand that the vendor has taken actions to mitigate the incident, including notifying law enforcement, successfully locking out the unauthorized users from their system, and undertaking a full forensic investigation of the incident. In addition, we have suspended all activity with this vendor. With respect to payment card data, we have notified Visa, Mastercard, American Express and Discover so that they may take appropriate action to protect cardholders. [redacted]

Further, to help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: February 28, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code** [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (855) 896-4451 by **February 28, 2021**. Please be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian. A credit card is not required for enrollment in Experian IdentityWorks.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

What You Can Do:

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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More information:

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (855) 896-4451. 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 (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 this Identity Restoration support is available to you for two years 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. You will also find self-help tips and information about identity protection at this site. You should also report any suspected incident of identity theft to law enforcement and you can obtain a copy of any resulting police report. You should also notify your state Attorney General and the FTC. [redacted]

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at (855) 896-4451.

Sincerely,

Bruce Stewart
President

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

[redacted]

Information on Obtaining Credit Reports, Credit Freezes and Security Alerts

It is important that you remain vigilant over the next 12 to 24 months by reviewing your account statements and monitoring your credit reports for suspicious activity. We have provided information below about how to contact the credit reporting agencies and the Federal Trade Commission to obtain your credit report, place fraud alerts and credit freezes, and obtain additional information.

Obtain a Free Credit Report: You may obtain a free copy of your credit report from each of the three nationwide consumer reporting agencies by calling 1-877-322-8228 or going online to www.annualcreditreport.com. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies.

Credit Freezes & Fraud Alerts: You have a right to place a 'security freeze' on your credit report at no charge, which will prohibit a credit reporting agency from releasing information in your credit report without your written authorization. The security freeze is designed to prevent credit loans, and services from being approved in your name without your consent. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prohibit the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other accounts involving the extension of credit. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 7 years.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. To place a security freeze on your credit report, you must contact **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Experian: (888) 397-3742 Experian Security Freeze P.O. Box 9554 Allen, TX 75013 https://www.experian.com/freeze/center.html	**Equifax: (877) 298-0045** Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 https://www.equifax.com/personal/credit-report-services/credit-freeze/	**TransUnion: (888) 909-8872** TransUnion Credit Freeze P.O. Box 160 Woodland, PA 19094 https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agencies, depending on whether you do so online, by phone, or by mail: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc.), (2) Social Security Number, (3) Date of birth, (4) If you have moved in the past five years, the addresses where you have lived over the prior five years, (5) 5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed, (6) a legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.), (7) Social Security Card, pay stub, or W2, (8) 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.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

[redacted]

To learn more about fraud alerts, security freezes, and protecting yourself from identity theft and to report incidents of identity theft, you can visit the Federal Trade Commission's website at www.consumer.gov/idtheft, or www.ftc.gov/credit, or call 1-877-IDTHEFT (1-877-438-4338). You may also receive information from the Federal Trade Commission by writing to: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You also have a variety of rights under the federal Fair Credit Reporting Act (FCRA). For more information on your FCRA rights, visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

For residents of the following states, your state's statute requires that we notify you that you may also obtain information about preventing and avoiding identity theft from your State Attorney General's Office or other state resource listed below:

- Maryland: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us
- North Carolina: North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov
- New York: New York Division of Consumer Protection, consumer hotline 800-697-1220, https://www.dos.ny.gov/consumerprotection/security_breach/data_security_breach.htm
- Rhode Island: RI Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400; http://www.riag.ri.gov/ConsumerProtection/About.php#
- Washington DC: Office of the Attorney General for the District of Columbia: https://oag.dc.gov/.

APPENDIX TO SAMPLE NOTIFICATION LETTER

Key to Extra Fields:

Extra1: Shortened name of company, i.e. "Direct Energy"

Extra2: Unique field for Rhode Island only

Extra3: "your bank account information" or "your credit card information" or "your credit card information together with your username and password" or "your username and password"

Extra 4: This field is only used if "your username and password" appears in Extra3

> "We have implemented a password change in our systems as precaution. The next time you log into your account with us you will be asked to reset your password. Please do so, and also change your password on other accounts if you have used the same login credentials for any other accounts."

Extra 5: This field is only used if "your bank account information" appears in Extra3.

> "Security Alert with ChexSystems: You may place an alert with ChexSystems. Chex Systems, Inc. is a consumer-reporting agency governed by the FCRA and other laws (the Federal Trade Commission enforces the FCRA) which provides account verification services to its financial institution members to aid them in identifying account applicants who may have a history of account mishandling (for example, people whose accounts were overdrawn and then closed by them or their bank). In short, ChexSystems is like the credit reporting agencies (Equifax, Experian, TransUnion) but specific to checking/savings history instead of credit/loan history. ChexSystems has two protections available:
>
> • Consumer Report Security Alert. This puts a flag on your consumer file stating the banking institution needs to take additional steps to confirm it is you who is initiating the action (much like placing a fraud alert with the credit reporting agencies). You may request a 90-day alert, which is the default, though you may extend it to 7 years if you complete the ChexSystems ID Theft affidavit form (available online), have the affidavit notarized, and send the notarized affidavit to ChexSystems. To set the Consumer Report Security Alert, call (888) 478-6536 or online by visiting https://www.chexsystems.com.
>
> • Consumer Report Security Freeze. This will prohibit ChexSystems from releasing any information in your consumer file without your express authorization, meaning you have to contact ChexSystems and lift the freeze in order for your information to be released (much like placing a freeze with the credit reporting agencies). You should be aware that taking advantage of this right may delay or prevent timely approval from any user of your consumer report that you wish to do business with. The third party will receive a message indicating that you have blocked your information. To set the

Consumer Report Security Freeze, call (800) 887-7652 or online by visiting https://www.chexsystems.com."

Extra6: This field is only used if "your credit card information" is in Extra 3.

"If you manage your account with us online and had a payment card stored for automatic payments on your account, you will need to update that with your new card information."