SheppardMullin

Sheppard, Mullin, Richter & Hampton LLP
501 West Broadway, 19th Floor
San Diego, California 92101-3598
619.338.6500 main
619.234.3815 fax
www.sheppardmullin.com

619.338.6619 direct
JPhillips@sheppardmullin.com

April 27, 2021

Via Email: attorneygeneral@doj.nh.gov

New Hampshire Attorney General's Office
33 Capitol St,
Concord, NH 03301

Re: NOTICE OF DATA INCIDENT

I am writing on behalf of Doosan Fuel Cell America, Inc. ("DFCA") regarding a data incident that impacted the personal information belonging to 8 New Hampshire residents.

Description of the Incident
DFCA's IT vendor informed DFCA on or about January 22 that it had detected suspicious activity related to some of its file servers. Those servers contained personal information of current/former employees and contractors of DFCA and its predecessors - ClearEdge Power, Inc. and United Technologies Corporation. DFCA's IT vendor immediately took steps to secure file servers, hired a third-party forensic investigator, and conducted an investigation into the nature and scope of the suspicious activity. The investigation determined that an unknown threat actor managed to access personal information between January 3, 2021 and January 22, 2021. Upon learning of this incident DFCA hired its own forensic investigator to analyze the personal information that may have been impacted.

Steps Taken to Remedy the Breach
Since learning of the incident DFCA has been working to understand what happened and to remedy the situation. DFCA worked with its IT vendor to implement global password resets, deploy additional security for privileged accounts, and take steps to remove the attackers from all systems. DFCA took steps to improve security around employee administrator accounts, and has worked with its IT vendor to implement multi-factor authentication for employee email accounts. DFCA has also worked with its IT vendor to install new security applications to detect and prevent suspicious activities on its networks. DFCA has also worked with its IT vendor to notify law enforcement of this incident.

On March 24 DFCA received the forensic investigator report detailing names of individuals potentially impacted. However more than 90% of the individuals in the report were missing addresses and contact information. DFCA conducted a manual search of its systems to attempt to locate contact information for these individuals but could not locate any addresses. DFCA retained a vendor to assist with locating current contact information for the impacted individuals. The vendor provided a report to DFCA with last-known contact information on April 14 for approximately 1,300 individuals. It was not until April 14 that DFCA knew individuals in New Hampshire were impacted. Notice was/will be mailed on April 27.

Please find a sample of the notice sent to New Hampshire residents below. If you have any questions about this notice or this incident, you can contact me directly at 619-338-6619 or JPhillips@sheppardmullin.com.

Very Respectfully,

Justine M. Phillips
for SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Doosan Fuel Cell America, Inc. ("DFCA") was informed by its IT vendor about a cybersecurity event that resulted in unauthorized access to some of its systems. DFCA is the successor to ClearEdge Power, Inc. ("ClearEdge Power") and the fuel cell business of United Technologies Corporation, ("UTC Power"). These systems may have included files that contained the personal information of some of DFCA's current and former employees, contractors, and ClearEdge Power and UTC Power employee data (collectively, "Personal Information"). Although we have no evidence of actual or attempted misuse of your information, this letter provides details of the incident, our investigation, and steps you can take in response.

What Happened? Our IT vendor informed DFCA that it detected suspicious activity related to some of its file servers. Our IT vendor immediately took steps to secure file servers, hired a third-party forensic investigator, and conducted an investigation into the nature and scope of the suspicious activity. The investigation determined that an unknown actor managed to access Personal Information between January 3, 2021 and January 22, 2021. Upon learning of this incident DFCA hired its own forensic investigator to analyze the Personal Information.

What Information Was Involved? The Personal Information may have included information you provided to DFCA, ClearEdge Power, or UTC Power when you were hired, such as <<b2b_text_1(DataElements)>>. Therefore, in an abundance of caution we are notifying you of this incident to help you take steps to protect against the possibility of identity theft and fraud. To date, DFCA has not received any reports of actual or attempted misuse of your information.

What We Are Doing. The confidentiality, privacy, and security of information is one of our highest priorities and we take this incident very seriously. Since learning of the incident we have been working to understand what happened and to remedy the situation. Our IT vendor implemented global password resets, deployed additional security for privileged accounts, and took steps to remove the attackers from all systems. DFCA took steps to improve security around employee administrator accounts, and worked with our IT vendor to implement multi-factor authentication for employee email accounts, and install new security applications to detect and prevent suspicious activities on its networks. We have also worked with our IT vendor to notify law enforcement.

As part of our ongoing commitment to privacy and security, we are working to review our existing policies and procedures, to implement additional safeguards, and to provide additional training to our employees on data privacy and security. We are also notifying state regulators as required.

As an added precaution, we are offering you complimentary access to two years of credit and identity monitoring, fraud consultation, and identity theft restoration services through our service provider Kroll. We encourage you to activate these services, as we are not able to act on your behalf to activate you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. We strongly encourage you review the enclosed *Steps You Can Take to Help Protect Your Information*, which contains information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate. You may also activate the free identity monitoring services we are offering.

For More Information. We sincerely regret any inconvenience or concern this incident has caused. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated call center at 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time excluding major U.S. holidays.

Sincerely,

Daniel Reynolds
Director of Human Resources

Doosan Fuel Cell America, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

*You have until **<<Date>>** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Additional Steps

Review Your Accounts For Suspicious Activity. 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. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission (the "FTC").

Free Copy of Credit Report. 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.

Security Freeze. 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

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

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 (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. 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.

Fraud Alert. 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.

Rights Under the Fair Credit Reporting Act (FCRA): You also have certain rights under the FCRA. These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

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.

State Attorneys General can be reached below:

- **California:**

  Attorney General's Office
  California Department of Justice
  P.O. Box 944255
  Sacramento, CA 94244-2550
  Tel: (800) 952-5225
  https://oag.ca.gov/
  Identity theft information sheets.

- **Connecticut:**

  Attorney General's Office
  55 Elm Street
  Hartford
  CT 06106
  Tel: 1-860-808-5318
  www.ct.gov/ag

- **Massachusetts:**

  Office of the Attorney General
  Consumer Advocacy & Response Division
  One Ashburton Place, 18th Floor
  Boston, MA 02108
  Tel: (617) 727-8400
  https://www.mass.gov/orgs/office-of-attorney-general-maura-healey

- **North Carolina:**

  Office of the Attorney General
  114 West Edenton Street
  Raleigh, NC 27603
  Tel: (919) 716-6400

- **Maryland:**

  Office of the Attorney General
  200 St. Paul Place
  Baltimore, MD 21202
  Tel: (410) 528-8662
  https://www.marylandattorneygeneral.gov/

- **Oregon:**

  Oregon Department of Justice
  1162 Court St. NE
  Salem, OR 97301-4096
  Tel: 1-877-877-9392