McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Colin M. Battersby
Direct Dial: 248-593-2952
E-mail: cbattersby@mcdonaldhopkins.com

May 26, 2020

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Florida Engineers Management Corporation – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Florida Engineers Management Corporation ("FEMC"). I am writing to provide notification of an inadvertent disclosure at FEMC that may affect the security of personal information of approximately five (5) New Hampshire residents. FEMC's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission. By providing this notice, FEMC does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On February 11, 2020, FEMC inadvertently disclosed a document containing the Social Security numbers of a group of licensed professional engineers in response to a public records request. Upon being alerted to the error by the recipient on April 1, 2020, FEMC immediately requested that the recipient delete the information in all forms and verify that it had not been shared with anyone, which the recipient did. FEMC's investigation concluded on April 27, 2020 that the document contained the names and Social Security numbers of five New Hampshire residents.

To date, FEMC has no evidence or reason to believe that the recipient's response was anything other than genuine, and does not know of any misuse of any person's information resulting from this incident. Nevertheless, out of an abundance of caution, FEMC wanted to inform you (and the affected residents) of the incident and to explain the steps it is taking to help safeguard the affected residents against identity fraud. FEMC will provide the affected residents with written notification of this incident commencing on or about May 27, 2020 in substantially the same form as the letter attached hereto. FEMC will provide the residents with 12 months of credit monitoring, and will advise the 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 will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At FEMC, protecting the privacy of personal information is a top priority. FEMC is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. FEMC continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions concerning this notification, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Colin M. Battersby

Encl.

FEMC
Florida Engineers Management Corporation

[redacted]

[redacted]

IMPORTANT INFORMATION

PLEASE REVIEW CAREFULLY

[redacted]

[redacted]

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Florida Engineers Management Corporation ("FEMC"). As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

On February 11, 2020, FEMC inadvertently disclosed a document containing the Social Security numbers of a group of licensed professional engineers in response to a public records request. Your Social Security number was included. Upon being alerted to the error by the recipient on April 1, 2020, FEMC immediately requested that the recipient delete the information in all forms and verify that it had not been shared with anyone, which the recipient did. FEMC's investigation into the incident concluded on April 27, 2020.

We have no evidence or reason to believe that the recipient's response to us was anything other than genuine, and we do not know of any misuse of anyone's information resulting from this incident. Nevertheless, we want to make you aware of the incident out of an abundance of caution. Additionally, we are offering you a complimentary one-year membership in *my*TrueIdentity provided by TransUnion Interactive, a subsidiary of TransUnion. For more information on identity theft prevention and *my*TrueIdentity, including instructions on how to activate your 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 account statements for fraudulent or irregular activity on a regular basis.

Please accept our apologies that this incident occurred. We are 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 and internal controls 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 to 9 pm EST.

Sincerely,

[redacted]

Florida Engineering Management Corporation

AA5061 v.03

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for one year. The service is called *my*TrueIdentity and provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at [redacted]. When prompted, enter the following 6-digit telephone pass code [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and [redacted]. Due to privacy laws, we cannot register you directly. Please note that credit monitoring service might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12 month credit monitoring services, you may place an initial 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	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. Consider 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. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/
1-800-685-1111	1-888-397-3742	securityfreeze
		1-888-909-8872

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 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.

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.

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: 1-888-743-0023.

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, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226.

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 (TDD/TYY Support: 800-788-9898).

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.