McDonald Hopkins
A business advisory and advocacy law firm®

STATE OF NH
DEPT OF JUSTICE
2017 APR 17 AM 11:50

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

James J. Giszczak
Direct Dial: 248.220.1354
jgiszczak@mcdonaldhopkins.com

April 3, 2017

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Forest City Trading Group, Inc. – Incident Notification

Dear Attorney General Delaney:

McDonald Hopkins PLC represents Forest City Trading Group, Inc. ("FCTG"). I write to provide notification concerning an incident that may affect the security of personal information of thirty six (36) New Hampshire residents. FCTG's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, FCTG does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On March 1, 2017, FCTG learned that equipment was stolen. Among the items stolen was a laptop that contained some information related to the employee stock ownership plan ("ESOP"). Upon learning of the situation, FCTG immediately commenced investigation, notified law enforcement, and engaged external cybersecurity professionals to analyze the extent of the compromise and assist in the response. Despite law enforcement's efforts, the laptop has not been recovered to date.

FCTG has devoted considerable time and effort to determine what exact information may have been contained in the laptop and, as such, may be at risk of disclosure. FCTG can confirm that the laptop contained information related to the ESOP, which included name, address, Social Security number, and date of birth.

To date, FCTG is not aware of any confirmed instances of identity fraud as a direct result of this incident. Nevertheless, FCTG wanted to make you (and the affected residents) aware of the incident and explain the steps FCTG is taking to help safeguard the residents against identity fraud. FCTG provided the New Hampshire residents with written notice of this incident commencing on March 31, 2017, in substantially the same form as the letter attached hereto. FCTG is offering the residents a complimentary membership with a credit monitoring and identity theft protection service. FCTG has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. FCTG has advised the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and

obtaining a free credit report. The residents also have been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

FCTG takes its obligation to help protect personal information very seriously. FCTG is continually evaluating and modifying its practices to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,

James J. Giszczak

Encl.

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

[redacted]

<<Date>>

Dear [redacted],

The privacy of your personal information is of utmost importance to [redacted]. I am writing to provide you with important information about a recent incident involving the security of some of your personal information that you supplied to us. We want to provide you with information regarding the incident and explain the services we are making available to help safeguard you against identity fraud. We also are providing additional steps you can take to help protect your information.

On March 1, 2017, we learned that equipment was stolen. Among the items stolen was a laptop that contained some information related to the employee stock ownership plan ("ESOP"). Upon learning of the situation, we immediately commenced investigation, notified law enforcement, and engaged external cybersecurity professionals to analyze the extent of the compromise and assist in our response. Despite law enforcement's efforts, the laptop has not been recovered to date.

We have devoted considerable time and effort to determine what exact information may have been contained in the laptop and, as such, may be at risk of disclosure. We can confirm that the laptop contained information related to the ESOP, which included your name, address, Social Security number, and date of birth.

To date, we are not aware of any reports of identity fraud or improper use of information as a direct result of this incident. Out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well.

Enclosed in this letter you will find information on enrolling in a 12-month membership of Equifax Credit Watch™ Gold, that we are providing at no cost to you, along with other precautionary measures you can take to help protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

Please accept our sincere apologies that this incident occurred. We are committed to maintaining the privacy of your information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of information.

If you have any further questions regarding this incident, please call [redacted] at [redacted] Monday through Friday, 9:00 a.m. to 5:00 p.m. Pacific Time.

Sincerely,

[redacted]

[redacted]

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

EQUIFAX®

Activation Code: [redacted]

About the Equifax Credit Watch™ Gold identity theft protection product	Equifax Credit Watch provides you with the following key features and benefits:
Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file. Note: You must be over age 18 with a credit file in order to take advantage of the product.	○ Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax** credit report ○ Wireless alerts and customizable alerts available (available online only) ○ Access to your Equifax Credit Report™ ○ Up to $25,000 in identity theft insurance with $0 deductible, at no additional cost to you † ○ Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance, and help initiate an investigation of inaccurate information. ○ 90 day Fraud Alert placement with automatic renewal functionality* (available online only)

How to Enroll: You can sign up online or over the phone

To sign up online for **online delivery** go [redacted]	To sign up for **US Mail delivery**, dial [redacted] for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.
1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button. 2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button. 3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button. 4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button. 5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.	1. Activation Code: You will be asked to enter your enrollment code as provided at the top of this letter. 2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number. 3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment. 4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

† Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. This product is not intended for minors (under 18 years of age).

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

You must sign-up for this credit monitoring before [redacted]. You will not be able to enroll after this date.

{6680442:}

2. **Placing a Fraud Alert.**

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "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**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
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**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-800-680-7289

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.

6. **Reporting Identity Fraud to the IRS.**

If you believe you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended you do the following:

- Contact your tax preparer, if you have one
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf.

- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm
- Report the situation to your local police or law enforcement department

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

7. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf.