JacksonLewis

Jackson Lewis P.C.
200 Connell Drive, Suite 3000
Berkeley Heights NJ 07922
(908) 795-5200 Direct
(908) 464-2614 Fax
jacksonlewis.com
Richard J. Cino – Managing Principal

STATE OF NH
DEPT OF JUSTICE
2021 JUL 29 AM 11:30

Mary T. Costigan, Esq.
Mary.costigan@jacksonlewis.com

July 20, 2021

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Security Incident

Dear Sir or Madam:

We represent Forest City Trade Group, LLC and its affiliated companies (collectively "FCTG"), located at 10250 SW Greenburg Road, Suite 300, Portland, OR. Pursuant to the N.H. Rev. Stat. §§359-C:19 *et seq.*[1], we are writing to notify you of a data incident.

On June 24, 2021, FCTG learned that it was the victim of an external cyber security attack that began on or about June 21, 2021, which may have resulted in the unauthorized access and acquisition of personal information of 142 New Hampshire residents. Upon discovering the attack, FCTG promptly notified the FBI and other applicable members of law enforcement. It also engaged a third-party cybersecurity firm to provide expert assistance with securing its systems, remediation efforts, and to perform a forensic investigation into the nature and scope of the incident. As part of these efforts, FCTG has deployed enterprise-wide endpoint monitoring solutions to detect any continued presence of the threat actors in its systems. FCTG is working diligently to identify how this incident occurred.

FCTG will be providing the affected individuals with written notice on or about July 21, 2021. In addition to advising the individuals on measures they can take to protect themselves, it has arranged for twenty-four-months of complimentary ID theft protection and monitoring services for adults and identity protection services for minor children. Please see attached letters.

FCTG continues to assess its security practices and will take step, as necessary, to minimize the risk of a similar incident occurring in the future. Should the company become aware of any significant developments concerning this situation, we will inform you.

[1] Please note that by providing this letter the Company is not agreeing to the jurisdiction of State of New Hampshire or waiving its right to challenge jurisdiction in any subsequent actions.

Please let us know if you have any questions.

Sincerely,
JACKSON LEWIS PC

/s/ Mary T. Costigan
Mary T. Costigan

Encl.

4848-5418-7505, v. 1

LETTERHEAD

Name
Address

Verification/Enrollment Code: [insert]

Date [insert]

Dear Parent or Guardian of [Name]:

Notice of Data Breach

Forest City Trading Group, LLC and its affiliated companies (collectively "FCTG") is sending this letter to notify you that we experienced a data incident that may have involved your minor child's personal information. In this letter, we describe what happened, how we are handling the situation, and who you can contact if you have any questions. At the end of this letter, we recommend precautionary measures you can take.

What Happened

On June 24, 2021, FCTG learned that it was the victim of an external cyber security attack that began on or about June 21, 2021 and may have resulted in the unauthorized access and acquisition of personal information.

What Information Was Involved

Although we are continuing to investigate the incident, we believe that data affected by the incident may include personal information we maintain in our systems for benefits purposes such as your minor child's name, address, and Social Security Number.

What We Are Doing

Upon discovering the attack, we promptly notified law enforcement. We also engaged a third-party cybersecurity expert to assist with securing our systems and our remediation efforts, and to perform a forensic investigation into the nature and scope of the incident. As part of these efforts, we have deployed enterprise-wide endpoint monitoring solutions to detect any continued presence of the threat actors in our systems. FCTG is working diligently to identify how this incident occurred. As we move through this process, we will continue to assess our security practices and take steps, as necessary, to minimize the risk of a similar incident occurring in the future.

Additionally, we would like to offer you complimentary First Watch Identity Protection Services on behalf of your minor child. **First Watch Identity Restoration** is automatically available to you with no enrollment required. If a problem arises, simply call [insert] and provide your Verification Code (listed above). Our recovery specialists will help bring your identity back to a "pre-theft" status.

First Watch Identity Protection, requires that you enroll. This includes Identity Risk Scores, Continuous Identity Monitoring, Account Activity Alerts, Dark Web Monitoring, $1 Million Identity Theft Insurance with $0 Deductible, Social Security Statement Access, Lost Wallet/Purse Assistance, Stop Credit Card Offers, Enewsletter and Monthly Email if No Suspicious Activity is found. If suspicious activity is found, First Watch will place a personal phone call to you (at the telephone number that you provide) to determine if the suspicious activity is potentially fraudulent.

You can enroll your child in this service between now and [insert] using the Verification Code (listed above). To enroll, go to [insert], click on the Verification Code button and follow the instructions. Or, call [insert] Monday through Friday between the hours of 9 a.m. and 5:30 p.m. EST.

Please save this letter in a safe place. Your Verification Code (listed above) is required when calling First Watch ID Customer Service.

What You Can Do

In addition to enrolling in the complimentary Identity Protection Services, as with any data incident, we recommend that you remain vigilant and consider taking these precautionary measures:

- Review your minor child's personal account statements;
- Monitor free credit reports;
- Report any suspicious activity on your child's accounts to the company or financial institution; and
- Immediately report any fraudulent activity or suspected identity theft to your local law enforcement, state attorney general, and/or the Federal Trade Commission.

For More Information

We regret any concern this incident may cause. Please call us at [insert] if you have any questions.

Sincerely,

_____

Karen Mitchell
Vice President, HR
Forest City Trading Group, LLC

Additional Actions To Help Reduce Chances of Identity Theft

We recommend that you consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information:

1. **Place a 90 day fraud alert on your credit file**

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the credit cannot verify that you have authorized this, the

request should not be satisfied. You may contact any one of the credit reporting companies below for assistance.

Experian: 1-888-397-3742; www.experian.com
TransUnion: 1-800-680-7289; www.transunion.com
Equifax: 1-800-525-6285; www.equifax.com

2. Place a security freeze on your credit

If you are concerned about becoming a victim of security fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report, which will prevent them from extending credit. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also accessed through each of the credit reporting companies and there is no charge.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	Trans Union Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to request a security freeze, you may 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.); and
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, if available.

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.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper

identification (name, address, and Social Security Number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and Social Security Number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

3. Order your free annual credit reports

Consider visiting www.annualcreditreport.com or call 877-322-8228 to order your free annual credit reports. 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 any incorrect information, contact the credit reporting company.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 2390	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(866) 510-4211	(866) 751-1323	(800) 888-4213
psol@equifax.com	databreachinfo@experian.com	https://tudatabreach.tnwreports.com/
www.equifax.com	www.experian.com/	www.transunion.com

4. Manage your personal information

Take steps that include carrying only essential documents with you, be aware of with whom you share your personal information, and shred receipts, statements, and other sensitive information.

5. Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

By calling toll-free 1-888-567-8688, you can obtain a form to remove your name from pre-approved credit card offers. You will need to share some personal information, such as your name, Social Security number and date of birth when you submit your request. For more information on opting out of prescreen offers of credit, please refer to:
http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre17.shtm

6. Use Tools from Credit Providers

Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on your credit cards and bank accounts for notice of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, contact your creditor or bank immediately and file an identity theft report with your local police and contact a credit reporting company.

7. Report suspected identity fraud

You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission.

8. To obtain additional information about identity theft and ways to protect yourself

Contact the Federal Trade Commission ("FTC") either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is: 877-436-4338, TTY 866-653-4261.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

In addition to the FTC, you also may contact your state's attorney general's office and the credit reporting agencies above to provide you with information about fraud alerts and security freezes.

Residents of Maryland: You may obtain information about preventing identity theft from the following source: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (410) 576-6491, and http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx.

Residents of New York: You may obtain additional information from the New York State Police, 1220 Washington Avenue, Building 22, Albany, NY 12226-2252 or https://www.troopers.ny.gov/ and the Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Suite 640, Albany, NY 12231, Phone: (800) 697-1220 and https://www.dos.ny.gov/consumerprotection/.

Residents of North Carolina: You may obtain information about preventing identity theft from the following source: Office of the Attorney General, 0001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, and www.ncdoj.gov/Home/ContactNCDOJ.aspx.

LETTERHEAD

Name
Address

Verification/Enrollment Code: [insert]

Date [insert]

Dear [Name]:

Notice of Data Breach

Forest City Trading Group, LLC and its affiliated companies (collectively "FCTG") is sending this letter to notify you that we experienced a data incident that may have involved your personal information. In this letter, we describe what happened, how we are handling the situation, and who you can contact if you have any questions. At the end of this letter, we recommend precautionary measures you can take to protect yourself.

What Happened

On June 24, 2021, FCTG learned that it was the victim of an external cyber security attack that began on or about June 21, 2021 and may have resulted in the unauthorized access and acquisition of your personal information.

What Information Was Involved

Although we are continuing to investigate the incident, we believe that data affected by the incident may include personal information we maintain in our systems such as your name, address, Social Security Number, and HSA bank account number.

What We Are Doing

Upon discovering the attack, we promptly notified law enforcement. We also engaged a third-party cybersecurity expert to assist with securing our systems and our remediation efforts, and to perform a forensic investigation into the nature and scope of the incident. As part of these efforts, we have deployed enterprise-wide endpoint monitoring solutions to detect any continued presence of the threat actors in our systems. FCTG is working diligently to identify how this incident occurred. As we move through this process, we will continue to assess our security practices and take steps, as necessary, to minimize the risk of a similar incident occurring in the future.

Additionally, we would like to offer you complimentary ID theft protection and monitoring services for two-years that include:

- Free Annual Credit Report Access and Reminder Service (All 3 Bureaus): Provides easy access to federally mandated free credit reports from Experian, Transunion, and Equifax, along with a reminder service to request reports every four months (if individual provides email address).

- Once Annual Bureau Credit Report and Score provided through TransUnion.

- Single Bureau Credit Monitoring with Email Alerts as Applicable: Monitors and alerts a consumer when certain types of new activity appear on the TransUnion credit file.

- First Watch ID Identity Monitoring with Proactive Phone Alerts: Proprietary algorithms search and monitor thousands of databases and 300 billion records (99% of U.S. adult consumers) searching for suspicious activity that could indicate the beginning steps of identity theft.

- High Risk Monitoring - Account Activity Alerts: Monitors participating banks, online retailers, telecom providers, health insurers, and more by looking for suspicious activity that could indicate the beginning steps of identity theft to both the consumer's current accounts and new accounts.

- $1,000,000 Identity Theft Event Insurance with $0 Deductible – Discovery Based: Provides up to $1,000,000 Identity Theft Event Expense Reimbursement Insurance ($0 deductible) on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

- Fully Managed Identity Restoration – U.S. Based (No Signup Required). Should identity theft occur, First Watch Technologies, Inc. works to restore the consumer's name to pre-identity theft status. This benefit has an unlimited service guarantee.

What You Can Do

In addition to enrolling in the complimentary ID theft protection and monitoring services, as with any data incident, we recommend that you remain vigilant and consider taking these precautionary measures:

- Review your personal account statements;
- Monitor free credit reports;
- Report any suspicious activity on your accounts to the company or financial institution; and
- Immediately report any fraudulent activity or suspected identity theft to your local law enforcement, state attorney general, and/or the Federal Trade Commission.

To Enroll in Complimentary ID Theft Protection and Monitoring Services

First Watch Identity Restoration is automatically available to you with no enrollment required. If a problem arises, simply call [insert] and provide your Verification Code (listed above). Recovery specialists will help bring your identity back to a "pre-theft" status.

To receive **Credit Monitoring and Identity Protection**, enrollment is required. You can sign up for this free service between now and [insert] using the Verification Code (listed above). To enroll, simply call [insert] Monday through Friday between the hours of 9 a.m. and 5:30 p.m. EST or go to [insert] click on the Verification Code button and follow the instructions.

Credit Monitoring through TransUnion offers you credit monitoring services with email alerts and a once annual credit report and score. Following enrollment, additional steps are required by you to activate your credit alerts and review your credit score and report.

Please save this letter in a safe place. Your Verification Code is required when calling First Watch ID Customer Service.

For More Information

We regret any concern this incident may cause you. Please call us at [insert] if you have any questions.

Sincerely,

_____

Karen Mitchell
Vice President, HR
Forest City Trading Group, LLC

Additional Actions To Help Reduce Chances of Identity Theft

We recommend that you consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information:

1. **Place a 90 day fraud alert on your credit file**

   An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the credit cannot verify that you have authorized this, the request should not be satisfied. You may contact any one of the credit reporting companies below for assistance.

   Experian: 1-888-397-3742; www.experian.com
   TransUnion: 1-800-680-7289; www.transunion.com
   Equifax: 1-800-525-6285; www.equifax.com

2. **Place a security freeze on your credit**

   If you are concerned about becoming a victim of security fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report, which will prevent them from extending credit. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also accessed through each of the credit reporting companies and there is no charge.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	Trans Union Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to request a security freeze, you may 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.); and
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, if you have one.

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.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and Social Security Number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and Social Security Number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

3. Order your free annual credit reports

Consider visiting www.annualcreditreport.com or call 877-322-8228 to order your free annual credit reports. 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 any incorrect information, contact the credit reporting company.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 2390	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(866) 510-4211	(866) 751-1323	(800) 888-4213
psol@equifax.com	databreachinfo@experian.com	https://tudatabreach.tnwreports.com/
www.equifax.com	www.experian.com/	www.transunion.com

4. Manage your personal information

Take steps that include carrying only essential documents with you, be aware of with whom you share your personal information, and shred receipts, statements, and other sensitive information.

5. Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

By calling 1-888-567-8688, you can obtain a form to remove your name from pre-approved credit card offers. You will need to share some personal information, such as your name, Social Security Number and date of birth when you submit your request. For more information on opting out of prescreen offers of credit, please refer to: http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre17.shtm.

6. Use Tools from Credit Providers

Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on your credit cards and bank accounts for notice of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, contact your creditor or bank immediately and file an identity theft report with your local police and contact a credit reporting company.

7. Report suspected identity fraud

You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission.

8. To obtain additional information about identity theft and ways to protect yourself

Contact the Federal Trade Commission ("FTC") either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is: 877-436-4338, TTY 866-653-4261.

Federal Trade Commission
Consumer Response Center

600 Pennsylvania Avenue
NW Washington, DC 20580

In addition to the FTC, you also may contact your state's attorney general's office and the credit reporting agencies above to provide you with information about fraud alerts and security freezes.

Residents of Maryland: You may obtain information about preventing identity theft from the following source: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (410) 576-6491, and http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx.

Residents of New York: You may obtain additional information from the New York State Police, 1220 Washington Avenue, Building 22, Albany, NY 12226-2252 or https://www.troopers.ny.gov/ and the Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Suite 640, Albany, NY 12231, Phone: (800) 697-1220 and https://www.dos.ny.gov/consumerprotection/.

Residents of North Carolina: You may obtain information about preventing identity theft from the following source: Office of the Attorney General, 0001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, and www.ncdoj.gov/Home/ContactNCDOJ.aspx

4833-2752-6385, v. 1