JacksonLewis

Jackson Lewis P.C.
6100 Oak Tree Blvd., Suite 400
Cleveland, OH 44131
(216) 750-4303 Main
(216) 750-0826 Fax
www.jacksonlewis.com

Jackson Biesecker
Direct: (216) 750-4303
jackson.biesecker@jacksonlewis.com

Office of the Attorney General
Department of Justice
Consumer Protection Bureau
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Incident Notification[1]

January 4, 2022

Dear Sir or Madam:

Please be advised that on November 2, 2021, our client, Wangs Alliance Corporation d/b/a WAC Lighting ("WAC"), learned that the personal information of two New Hampshire residents may have been subject to unauthorized access or acquisition as the result of a cyberattack (the "Incident").

Based on the underlying investigation, it appears the Incident occurred on or around March 11 to November 2, 2021. The data elements involved may have included a name, address, birth date, social security number, passport information, and in some circumstances a credit card number.

Immediately upon learning about the Incident, WAC commenced an investigation to determine the scope of the Incident and identify those potentially affected. This included WAC working with its information technology team and third-party forensic experts in an effort to ensure the Incident did not result in any additional exposure of personal information and to determine what information may have been accessed or acquired.

In light of this Incident, WAC plans to begin notifying individuals in the next several days. A draft copy of the notification that will be sent is enclosed with this letter.

As set forth in the enclosed letter, WAC has taken steps to protect the security of the personal information of all individuals. In addition to continuing to monitor this situation,

[1] Please note that by providing this letter WAC is not agreeing to the jurisdiction of State of New Hampshire, nor waiving its right to challenge jurisdiction in any subsequent actions.

WAC is reexamining its current privacy and data security policies and procedures to minimize the chances of this happening again. WAC has performed a global password reset and deployed endpoint detection and response software throughout the enterprise. Should WAC become aware of any significant developments concerning this situation, we will inform you.

If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS, P.C.
/s/ Jackson Biesecker
jackson.biesecker@jacksonlewis.com
6100 Oak Tree Blvd., Suite 400
Cleveland, OH 44131
PH: (216) 750-4303
FX: (216) 750-0826

JACKSON LEWIS, P.C.
/s/ Joe Lazzarotti
joe.lazzarotti@jacksonlewis.com
200 Connell Drive, Suite 2000
Berkeley Heights, NJ 07922
PH: (908) 795-5205
FX: (908) 464-2614

WAC Lighting
10300 SW Greenburg Rd. Ste. 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 4, 2022

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

WAC Lighting ("WAC") experienced a cybersecurity attack that may have involved your personal information. Fortunately, the attack was addressed quickly by our IT department working alongside a world-class cyber security firm and there was minimal interruption to our business. While we have reason to believe that the breach was contained, we are doing everything we can to protect our systems and implement additional measures to prevent a similar event in the future.

What Happened

WAC learned it was the subject of a cybersecurity attack occurring from March 11 to November 2, 2021. On November 2, 2021 the attackers deployed malware causing the encryption of a number of network drives and back-ups. We promptly took steps to secure our network and our third-party cybersecurity firm is conducting a forensic investigation into the cause and scope of the attack.

What Information Was Involved

At this time, we have no indication that any personal information was downloaded or used to commit identity theft or fraud. However, **out of an abundance of caution,** we feel it would be wise to inform you of the potential that certain elements of personal information could have been compromised in the attack. These data elements may have included a name, address, Social Security Number or other tax ID number, Passport information, or credit card number. We are providing this notice so that you can take any precautions you may deem necessary.

What We Are Doing

WAC endeavors to protect the privacy and security of personal information and we are taking aggressive measures to prevent a similar situation in the future. In response to the attacks, WAC changed passwords, deployed an end point monitoring solution, and began the process of upgrading its virus and malware protections.

While at this time, there is no evidence that your information has been misused or is even in possession of the attackers, out of an abundance of caution, we have arranged for ID theft and credit monitoring services to help mitigate any potential for harm at no cost to you. Please see below for more information on enrollment.

What You Can Do

As with any data incident, we recommend that you remain vigilant and consider taking steps to avoid identity theft, obtain additional information, and protect your personal information. Common passwords or passwords you may be using on

multiple accounts should be updated to new complex passwords for added security. The attached sheet describes steps you can take to protect your identity and personal information.

We are offering identify theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include <<12 months/24 months>> of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this specialized protection, IDX can help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4710 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 am to 9:00 pm Eastern Time. Please note the deadline to enroll is April 4, 2022.

Again, at this time, there is no evidence that your information has been stolen or that the attackers have successfully acquired it. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

WAC Lighting takes this incident seriously as cyber attacks are rising all over the world. Be assured that we are taking aggressive steps to minimize the chances of a similar occurrence. We understand that you may have more questions. Please feel free to call 1-800-939-4170 for more personalized assistance on the matter.

Warmly,

Shelley Wald
Co-CEO

(Enclosure)

Generally Recommended Steps to Help Further Protect Your 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 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. 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
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
www.equifax.com	www.experian.com	www.transunion.com

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

   - Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
   - Social Security Number;
   - Date of birth;
   - If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
   - Proof of current address such as a current utility bill or telephone bill;
   - A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
   - 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.

   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. Visit www.annualcreditreport.com or call 877-322-8228 to obtain a free annual credit report. Once you receive your credit report, review it for discrepancies, identify accounts you did not open or inquiries from creditors that you did not authorize, and 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	speakup@transunion.com
www.equifax.com	www.experian.com/	www.transunion.com

4. Use tools from credit providers and monitor your statements. 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, file an identity theft report with your local police and contact a credit reporting company. We also recommend that you review the statements you receive from your healthcare provider and health insurer. If you see any charges for services that you did not receive, please call the provider or insurer immediately.

5. Report suspected identity theft. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, the Attorney General, or the Federal Trade Commission.

6. **Residents of California**: Visit the California Office of Privacy Protection for additional information on protection against identity theft at www.oag.ca.gov/privacy.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: 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.

New York Residents: 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/.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer

Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: 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.

Rhode Island Residents: you can obtain information from the Rhode Island Attorney General about steps you can take to help prevent identity theft at: RI Office of Attorney General, 150 South Main St., Providence, RI 02903, Phone: (401) 274-4400 and consumers@riag.ri.gov.

7. To contact the FTC, or for additional information on identity theft, please call or contact the FTC at 877-436-4338, TTY 866-653-4261.

www.ftc.gov/idtheft.
Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580