LEWIS BRISBOIS BISGAARD & SMITH LLP

Elizabeth R. Dill
550 E. Swedesford Road, Suite 270
Wayne, PA 19087
Elizabeth.Dill@lewisbrisbois.com
Direct: 215.977.4101

July 22, 2020

VIA EMAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

I represent American Public Works Association ("APWA"), a non-profit membership organization that serves public works professionals, located in Kansas City, Missouri. This letter is being sent pursuant to N.H. Rev. Stat. §§ 359-C:19 - C:21 because APWA learned on July 13, 2020 that the payment card information of four (4) New Hampshire residents may have been involved in a data security incident. The affected information involved includes names, payment card numbers, expiration dates and security codes.

APWA maintains an online store (www.apwa.net), through which members can, *inter alia*, pay dues, purchase access to online training and educational events. On May 19, 2020, APWA learned of suspicious activity occurring in its online store. APWA took immediate steps to secure its system and member information, and launched an internal investigation. APWA thereafter engaged and worked with a nationally-recognized digital forensics firm to determine what happened as well as whether, and to what extent, the payment card information of APWA customers had been compromised. APWA also immediately reported the incident to the payment card brands in order to protect the affected individuals' payment card information and prevent fraudulent activity. APWA also reported the incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators accountable.

On June 23, 2020, APWA's investigation determined that the payment card information of customers of APWA who made purchases through APWA's online store between April 10, 2020 and May 20, 2020 was potentially compromised by the incident. On July 13, 2020 APWA confirmed that four (4) of these individuals are residents of New Hampshire.

On July 20, 2020, APWA notified the affected New Hampshire residents with the attached letter. As referenced in the letter, American Public Works Association will provide 12 months of identity protection services through ID Experts. Please do not hesitate to contact me should you have any questions.

Sincerely,

Elizabeth R. Dill of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Consumer notification letter

C/O ID Experts
10300 SW Greenburg RD Suite 570
Portland, OR 97223

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

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

July 20, 2020

Notice of Data Security Incident

Dear <<FirstName>> <<LastName>>,

The American Public Works Association ("APWA") is writing to notify you of a data security incident relating to your purchase through our online store (www.apwa.net/store/) that may have involved your payment card information. At APWA, we take the privacy and security of your information very seriously. We are writing to both inform you of the incident, and to advise you about certain steps you can take to protect your information.

What happened? On May 19, 2020, we learned of suspicious activity occurring in our online store. Upon discovering the activity, we took immediate steps to secure our system and member information. We also immediately took steps to investigate the situation. APWA retained and worked with a leading forensics firm to investigate whether any member information had been accessed or acquired without authorization. We recently received a determination from the forensic investigation that certain payment card information may have been exposed as a result of unauthorized activity in the online store.

What information was involved? The unauthorized access to our online store potentially compromised payment card information belonging to customers who made purchases through our online store between April 10, 2020 and May 20, 2020. The payment card information that may have been compromised included names, card numbers, expiration dates, and security codes.

What we are doing. As soon as we discovered the incident, we took the steps described above. In addition, we immediately reported the matter to the payment card brands to protect your payment card information and prevent fraudulent activity. We have also reported the incident to the Federal Bureau of Investigation, and will provide whatever cooperation is necessary to hold the perpetrators accountable.

As an added precaution, we are offering, at no cost to you, identity theft protection services through ID Experts.® Your MyIDCare™ services include: 12 months of CyberScan monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What you can do. You can follow the recommendations included with this letter to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent

transactions have taken place, you should call the bank that issued the card immediately. We encourage you to contact ID Experts with any questions and to enroll in the complimentary MyIDCare services by calling 1-800-939-4170 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is July 20, 2020.

For more information. Detailed instructions for enrollment in the MyIDCare services are provided in the enclosed Recommended Steps document. When you enroll by phone or online, you will need to reference your enrollment code, located at the top of this letter. Please call 1-800-939-4170 or go to https://app.myidcare.com/account-creation/protect for assistance or for any additional questions you may have.

We take this matter very seriously. Please accept our sincere apologies for any concern or inconvenience that this incident may cause you.

Sincerely,

Scott D. Grayson, CAE
Chief Executive Officer
American Public Works Association
1200 Main Street, Suite 1400
Kansas City, MO 64105-2100

MyIDCare

Recommended Steps to Protect your Information

1. **Website and Enrollment.** Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. CyberScan will be automatically activated upon enrolling. You may login to your membership to add additional information into CyberScan. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that 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 or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

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

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 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.