

Samantha L. Southall
215 665 3884
samantha.southall@bipc.com

Two Liberty Place
50 S. 16th Street, Suite 3200
Philadelphia, PA 19102-2555
T 215 665 8700
F 215 665 8760

February 24, 2022

VIA U.S. MAIL

Attorney General Lawrence G. Wasden
Office of the Attorney General
State of Idaho
700 West Jefferson Street
P.O. Box 83720
Boise ID 83720-0010

Re: *Security Breach Incident*

Dear Attorney General Wasden:

We are submitting this notification on behalf of the Washington State Department of Licensing (“DOL”) pursuant to Idaho Code § 28-51-104 *et seq.* DOL recently experienced unauthorized access to its Business and Professional License System (the “B&P System”). The B&P System includes information for licenses issued by DOL as well as the Board of Registration for Professional Engineers & Land Surveyors. Based upon its investigation, DOL believes the personal data of 6,909 Idaho residents was involved.

On January 24, 2022, DOL became aware that data, which appeared to come from the B&P System, had been accessed without authorization. DOL immediately took the B&P System offline and alerted the service providers involved in hosting the B&P System. DOL also has been working with its service providers, Washington Technology Solutions and a nationally recognized cybersecurity expert to conduct a detailed forensic analysis. Law enforcement also is involved. No suspicious activity has been detected in any other system operated by DOL, including the drivers’ and vehicle license system, all of which are being monitored.

DOL is implementing additional safeguards to protect the B&P System. As soon as it is safe and appropriate, the B&P System will be brought back online. To limit the impact on licensees whose licenses expire during the outage, DOL is automatically waiving all late-filing penalties through April 1, 2022. In addition, DOL is implementing protocols to process those renewals paused by the outage more quickly.

The investigation revealed that personal information in DOL professional or business license records may have been obtained by an unauthorized actor. The affected information may

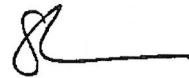
February 23, 2022

Page - 2 -

have included licensees' names, e-mail addresses, Social Security numbers, dates of birth, and/or driver's license numbers.

DOL will be providing notice to all affected individuals. Enclosed please find a copy of the notice letter that will be sent to the affected individuals. If you have any questions or would like additional information, do not hesitate to contact me.

Very truly yours,

A handwritten signature in black ink, consisting of a stylized initial 'S' followed by a horizontal line.

Samantha L. Southall

Enclosure



STATE OF WASHINGTON
DEPARTMENT OF LICENSING

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Activation Code: <<Activation Code s_n>>

Re: Important Data Security Notification from the Washington Department of Licensing

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

You are receiving this letter because you have a business or professional license or have provided information to the Business and Professional License System (the “B & P System”) operated by the Washington State Department of Licensing (“DOL”). The B&P System includes information for licenses issued by both DOL and the Board of Registration for Professional Engineers & Land Surveyors (BRPLES).

DOL has determined that personal information in your license record in the B&P System was exposed to unauthorized activity. Depending on the type of license you hold, the exposed information may include your name, e-mail address, Social Security number, date of birth, and/or driver’s license number. While we are investigating how this happened, it is most important that we get this notice to you without delay. To help you protect your information, we are offering you one year of free credit monitoring and identity theft protection services.

What Happened?

On January 24, 2022, DOL became aware that data, which appeared to come from the B & P System, had been accessed without authorization. We immediately took the B&P System offline and alerted the service providers involved in hosting the B&P System. We commenced a thorough investigation into how this occurred and engaged a nationally recognized cybersecurity expert to conduct a detailed forensic analysis.

No suspicious activity has been detected in any other system operated by DOL, including the drivers’ and vehicle license system, all of which are being closely watched.

What Information Was Involved?

We have learned that personal information in your DOL professional or business license record may have been obtained by an unauthorized person. Depending on the type of license you hold, the affected information may include your name, e-mail address, Social Security number, date of birth, and/or driver’s license number.

What Are We Doing?

DOL immediately took the B&P System offline to protect the information of our professional and occupational license holders. We are working with our service providers, the Washington Technology Solutions (WaTech), and a nationally recognized cybersecurity expert to conduct a thorough investigation into the incident. Law enforcement is also involved. The investigation is helping us determine the source of the unauthorized activity and the individuals who may have been impacted, so we can provide assistance to them. We are implementing additional safeguards to protect the B&P System. As soon as it is safe and appropriate, the B&P System will be brought back online.

To limit the impact on licensees whose licenses have expired during our outage, we are automatically waiving all late-filing penalties through April 1, 2022. In addition, we are implementing protocols to process those renewals paused by the outage more quickly. For detailed information about pending license questions, please visit our website at: www.dol.wa.gov/outage.

What We Recommend

We take the security of the personal information licensees entrusted to us very seriously. This letter contains specific instructions for how to sign up for credit monitoring with Experian, and we encourage you to take advantage of Experian's monitoring product and identity restoration service, which are provided to you free of charge.

We deeply regret the concern and inconvenience this matter may cause you. If you have any questions, please contact our call center at (855) 568-2160 Monday-Friday 8:00 AM – 5:00 PM Pacific Time (excluding major U.S. holidays) or visit www.dol.wa.gov/outage.

Sincerely,

The Washington State Department of Licensing
P.O. Box 9020
Olympia, Washington 98507-9020

IDENTITY RESTORATION SERVICES—NO ENROLLMENT NEEDED

Identity Restoration assistance is immediately available to you through Experian. You do not need to enroll. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. Be prepared to provide **engagement number** <<b2b_text_1(engagement number)>> as proof of eligibility for the Identity Restoration services by Experian.

If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that the Identity Restoration service is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

HOW TO ENROLL IN EXPERIAN IDENTITYWORKS

How to Enroll

We encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary one year membership. This product provides you with identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** <<b2b_text_6(activation deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://experianidworks.com/3bcredit>
- Provide your **activation code**: <<Activation Code s_n>>
- Provide your **engagement number**: <<b2b_text_1(engagement number)>>

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-855-870-5271 by <<b2b_text_6(activation deadline)>>. Be prepared to provide engagement number <<b2b_text_1(engagement number)>> as proof of eligibility for the Identity Restoration services by Experian.

Additional Details Regarding Your One Year Experian Identityworks Membership

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized **electronic** fund transfers.

ADDITIONAL STEPS TO HELP PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission ("FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to place a security freeze on your credit file. This will prevent new credit from being opened in your name without your express authorization. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to your state Attorney General.

Federal Trade Commission (FTC): The FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and, TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them as explained on their website. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

Fair Credit Reporting Act (FCRA): 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 violators. 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. We encourage you to 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.

For California residents: You may visit the California Office of Privacy Protection at www.oag.ca.gov/privacy for additional information on protection against identity theft.

For Kentucky residents: You can contact the State Attorney General at the Office of the Attorney general of Kentucky, Frankfort, Kentucky 40601; 502-696-5300; or at www.ag.ky.gov.

For Maryland residents: You can contact the State Attorney General at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov.

For 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 violators. 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. We encourage you to 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.

For North Carolina residents: You can contact the State Attorney General at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Oregon residents: You can contact the State Attorney General at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 877-877-9392; and online at <https://www.doj.state.or.us/>.