Appendix

The Washington State Department of Licensing ("DOL") recently learned of a website spoofing scam targeting individuals who use Secure Access Washington ("SAW"), Washington's portal to access online services provided by state agencies. Website spoofing is a scam that involves creating a website that is virtually identical to the authentic website with the goal of scamming individuals into sharing sensitive information – such as login credentials. As a result, between October 25, 2023, to November 20, 2023, individuals who entered their login credentials on one of these spoofed websites may have unknowingly provided their SAW login credentials to unauthorized individuals.

Upon discovering the incident, the State immediately launched an investigation with the assistance of multiple Washington State agencies and a third-party forensic specialist, to determine the nature and scope of the incident. Through the investigation, DOL identified certain data that the unauthorized individuals accessed during the incident.

DOL began a review of that data and, on January 16th, 2024, identified that the data contains the personal information of 997 Washington residents including the individual's name and driver's license number.

Beginning on January 30, 2024, DOL began mailing notification letters via United States Postal Service First-Class mail to the Washington residents, in accordance with Wash. Rev. Code § 19.255.010. A copy of the notification letter is enclosed. DOL has established a dedicated, toll-free call center to answer questions that individuals may have. DOL is also offering complimentary credit monitoring and identity theft protection services to eligible individuals and has encouraged the individuals to remain vigilant by reviewing their credit reports and account statements for any unauthorized activity.

To help prevent a similar incident from occurring in the future, DOL is implementing several changes to enhance its existing security measures.

STATE OF WASHINGTON
DEPARTMENT OF LICENSING
PO Box 9020 • Olympia, Washington 98507-9020

<<Name1>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<ZIP>>

<<Maildate>>

NOTICE OF DATA BREACH

The Department of Licensing writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so. The incident involved online accounts maintained by multiple Washington State agencies and, as a result, you may receive a similar letter from other State agencies related to the incident.

What Happened? We recently learned of a website spoofing scam targeting individuals who use Secure Access Washington ("SAW"), Washington's portal to access online services provided by state agencies. Website spoofing is a scam that involves creating a website that is virtually identical to the authentic website with the goal of scamming individuals into sharing sensitive information – such as login credentials. As a result, between October 25, 2023, and November 20, 2023, individuals who entered their login credentials on one of these spoofed websites may have unknowingly provided their SAW login credentials to unauthorized individuals. The State immediately launched an investigation with the assistance of multiple Washington State agencies and a third-party forensic specialist, to determine the nature and scope of the incident. We then reviewed contents of the affected SAW accounts to determine what, if any, sensitive information was contained within them. On January 16, 2024, our investigation determined that certain information in your Department of Licensing account may have been accessed and visible to an unauthorized individual.

What Information Was Involved? We determined that the unauthorized individuals may have viewed the following personal information related to you that was present in your Department of Licensing account at the time of the incident: name and driver's license number.

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. Once we became aware of the spoofing websites, we engaged cybersecurity and forensic teams to investigate the nature and scope of the incident. We are taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security. We have also arranged for you to receive a complimentary membership in Experian® IdentityWorks℠ Credit 3B. These identity protection services include one year of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. These services are completely free to you, and enrolling in this program will not hurt your credit score.

What You Can Do. You should promptly change your password and any security answer associated with your SAW account. You can also activate the complimentary identity monitoring services through Experian®. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. For more information on identity protection and steps you can take in response, please see the additional information provided with this letter.

Your confidence and trust are important to us. We regret that this occurred and apologize for any inconvenience this incident may have caused. If you have any questions, please call (888) 368-7291, Monday through Friday, 8:00 a.m. to 5:00 p.m., Pacific Time.

Sincerely,

Marcus J. Glasper
Director

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 12 months.

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. 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 Identity Restoration is available to you for 12 months 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [redacted] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: [redacted]

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 1-877-288-8057 by 4/28/2024. Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH 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.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.