

# BakerHostetler

## Baker&Hostetler LLP

811 Main Street  
Suite 1100  
Houston, TX 77002-6111

T 713.751.1600  
F 713.751.1717  
www.bakerlaw.com

Lynn Sessions  
direct dial: 713.646.1352  
lsessions@bakerlaw.com

May 5, 2025

### VIA EMAIL (SECURITYBREACH@ATG.WA.GOV)

Office of the Attorney General  
1125 Washington St SE  
Olympia, WA 98504

*Re: Supplemental Incident Notification*

Dear Sir or Madam:

On behalf of our client, Klickitat Valley Health (“KVH”), we are writing to update you regarding the incident that we initially reported to your office on March 14, 2025. Following the initial report, KVH’s ongoing review identified additional individuals whose information was involved in this incident. On May 2, 2025, KVH mailed letters to approximately 11,522 additional Washington residents, for a total of 11,960 Washington residents.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Lynn Sessions

## Appendix

On February 23, 2025, Klickitat Valley Health (“KVH”), a covered entity under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), identified unusual activity affecting its IT systems. KVH immediately took steps to contain the incident and began an investigation, which included assistance from external cybersecurity experts. KVH also reported the incident to law enforcement. The investigation determined that on February 18, 2025, an unauthorized third party obtained copies of certain files from KVH’s systems.

KVH is conducting a thorough review of the files involved, which is ongoing. Based on the review completed to date, the information involved may include name, date of birth, Social Security number, health insurance information, or medical information.

On March 14, 2025, KVH began mailing notification letters to 438 Washington residents via U.S. First-Class mail in accordance with HIPAA (45 CFR §§ 160.103 and 164.400 *et seq.*).<sup>1</sup> A sample copy of the notification letter is attached. KVH is offering eligible individuals whose Social Security number may have been involved a complimentary membership to credit monitoring and identity protection services. KVH has also established a dedicated call center where all individuals may obtain more information regarding the incident. KVH is continuing to assess the information involved and expects to mail letters to additional individuals in the coming weeks. KVH will update this report when notifications are complete.

KVH considers the health, safety, and privacy of its patients a top priority. KVH continuously updates and enhances systems to protect the data it maintains and to help prevent events such as this from occurring in the future.

---

<sup>1</sup> KVH is notifying your office of this incident in accordance with Wash. Rev. Code § 19.255.010.



Secure Processing Center  
25 Route 111, P.O. Box 1048  
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

\*\*\*Postal IMB Barcode

<<Date>>

Dear <<Full Name>>,

Klickitat Valley Health is committed to protecting the privacy and security of our patients' information. With that in mind, we are writing to make you aware of an incident involving some of your information. This letter includes information about the incident, steps we have taken in response, and offers steps you may consider taking.

**What Happened?** On February 23, 2025, KVH identified unusual activity affecting our IT systems. We immediately took steps to contain the incident and began an investigation, which included assistance from external cybersecurity experts. We also reported the incident to law enforcement. The investigation determined that on February 18, 2025, an unauthorized person obtained copies of certain files from our systems.

**What Information Was Involved?** Our ongoing investigation determined that some of your information may have been involved, such as your name, address, date of birth, Social Security number, health insurance information, medical record number, patient account number, as well as information related to care received at KVH, such as date(s) of service, physician name and department, diagnosis or other treatment information.

**What We Are Doing & What You Can Do.** While, to date, KVH is not aware of any patient information being used for identity theft or fraud, as a precaution, we are offering you a complimentary one-year membership in Experian® IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks<sup>SM</sup> is completely free to you, and we understand that enrolling in this program will not hurt your credit score. We also recommend that you review the statements you receive from your healthcare providers and health insurer. If you see services you did not receive, please call the provider or insurer immediately. For more information on identity theft prevention and IdentityWorks<sup>SM</sup>, including instructions on how to activate your complimentary membership and information about identity protection, please see the additional information provided with this letter.

We deeply regret any concern this incident may cause and want to assure you that we are committed to the security of our systems, and we remain ready to provide the high-quality care that you and your family have come to expect from KVH. Additionally, we are continually enhancing the security of our electronic systems and the data we maintain to help prevent events such as this from occurring in the future.

**For More Information.** If you have questions about this incident, please call 1-855-374-7069, Monday through Friday, between 6:00 a.m. and 6:00 p.m. Pacific Time.

Thank you for your longstanding support of KVH. We look forward to continuing to provide high-quality care to you and all of our patients.

Sincerely,

Jonathan Hatfield  
Chief Executive Officer

## Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. VISIT the Experian IdentityWorks website to enroll: [www.experianidworks.com/3bcredit](http://www.experianidworks.com/3bcredit)
3. PROVIDE the Activation Code: <<Activation Code>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877.288.8057** by <<Enrollment Deadline>>. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877.288.8057**. 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 (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 this Identity Restoration support 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](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

\* 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](http://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](http://www.equifax.com), 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-833-799-5355

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](http://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](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://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.

**Additional information for residents of the following states:**

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)