

August 19, 2025

*Via Online Form*

State of Washington  
Office of the Attorney General  
The Honorable Nick Brown  
Attorney General  
1125 Washington St. SE  
Olympia, WA 98504

Re: Hulberg and Associates, Inc. Notice of Data Breach

Dear Mr. Brown:

We are writing on behalf of our client, Hulberg and Associates, Inc. ("Hulberg and Associates") regarding a security incident. Hulberg and Associates, Inc., provides real estate appraisals and related services.

On July 11, 2025, Hulberg and Associates experienced suspicious activity on a company server. Hulberg and Associates' IT immediately commenced its incident response to isolate and contain the threat, including disconnecting the affected server from the network. Hulberg and Associates also engaged a cybersecurity firm to conduct a forensic investigation into the incident.

Based on the investigation, an unknown third party gained unauthorized access to Hulberg and Associates' company server that stores human resources ("HR") files. HR files containing certain personal information of current and former employees and independent contractors may have been compromised.

There was one (1) Washington resident impacted by the incident. A notification letter to that individual was mailed today on Tuesday, August 19, 2025. A sample of that notification letter is submitted online with this letter. Though Hulberg and Associates does not have evidence that any personal information has been fraudulently used as a result of the incident, Hulberg and Associates is offering impacted individuals twelve (12) months of free credit and identity monitoring services, including identity restoration services through Experian IdentityWorks<sup>sm</sup>.

*Go to next page . . .*

Washington Attorney General  
Hon. Nick Brown  
August 19, 2025  
Page 2

In addition, in its written notification, Hulberg and Associates provides impacted individuals detailed information and steps they can take to protect themselves and their personal information from identity theft and fraud.

Hulberg and Associates has taken several steps to contain the incident and enhance its security including changing all passwords, installing upgraded endpoint detection sensors on computers, and using a managed detection and response service, which is monitored 24/7 by a third-party security operations service, to monitor, detect and respond immediately to any threats to the company's network security.

Hulberg and Associates takes this incident, and the privacy and security of personal information, very seriously. If you have any questions or require further information, please feel free to contact me at [stephanie@sosparkslaw.com](mailto:stephanie@sosparkslaw.com) or by my office phone, (408) 207-4701, and I will respond as soon as possible.

Very truly yours,

**SPARKS LAW APC**



Stephanie O. Sparks, Esq.  
CEO

SOS:ss


Encl.

Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

August 19, 2025



N7872-L01-0000001 P001 T00001 \*\*\*\*\*SCH 5-DIGIT 12345  
SAMPLE A SAMPLE - L01 ALL STATES  
APT ABC  
123 ANY STREET  
ANYTOWN, ST 12345-6789

A barcode consisting of vertical bars of varying heights, representing the alphanumeric data from the previous lines. The bars are arranged in groups corresponding to different parts of the address and zip code.

**RE: Notice of Data Breach**

Dear Sample A. Sample:

We are writing to let you know about a security incident involving certain of your personal information. This notice explains what happened, what information may have been affected, what measures we are taking in response, and steps you can take to help protect yourself and guard against possible identity theft and fraud.

**What Happened?** On July 11, 2025, we experienced suspicious activity on a server at Hulberg and Associates, Inc. We immediately took measures to contain the incident, including disconnecting the affected server from the network, changing passwords, and upgrading our endpoint detection solution on company computers to monitor, detect and respond to threats to our network security. We engaged a cybersecurity firm to conduct a forensic investigation into the incident.

An unknown third party gained unauthorized access to a server that stores Hulberg and Associates' human resources files. Your personal information may have been exposed during the incident. Below, we describe what information may have been involved, what we are doing in response to the incident, and what you can do to be proactive and protect yourself.

**What Information Was Involved?** The server impacted stored records of current and former employees and independent contractors, including name, address, social security number, driver's license, identification card, passport or other government identification numbers, date of birth, and bank routing and account numbers used for direct deposits. However, we do not collect or store any security code, access code or password that would permit access to an individual's bank or other financial account. We also do not collect or store your full credit card numbers.

**What Are We Doing?** As noted above, as soon as we were alerted to suspicious activity, we took immediate measures to contain the incident, including disconnecting the affected server from the network, changing passwords, and upgrading our end point detection solution on company computers to monitor, detect and respond to threats to our network security. Further, we have secured the services of **Experian IdentityWorks**<sup>SM</sup> to provide you credit monitoring and identity theft restoration services at no cost to you, as described below.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks<sup>SM</sup> 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](http://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 November 28, 2025**, by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

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 toll free by November 28, 2025, at 833-745-2452, Monday – Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

#### **ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP**

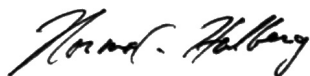
A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file 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.

**What You Can Do.** Please review the enclosed *Information about Identity Theft Protection* on how to protect against identity theft and fraud. Please remember to stay vigilant to avoid identity fraud. Take advantage of the complimentary identity protection services offered through Experian described above.

**For More Information.** We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-745-2452, toll free Monday through Friday from 8 am to 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE#.

Sincerely,



**Norm Hulberg, President**  
Hulberg and Associates, Inc.  
1530 The Alameda  
San Jose, CA 95126

\* 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.

## **Information about Identity Theft Protection**

### **Monitor Your Accounts**

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

**Equifax®**  
P.O. Box 740241  
Atlanta, GA 30374-0241  
1-800-685-1111  
[www.equifax.com](http://www.equifax.com)

**Experian**  
P.O. Box 2002  
Allen, TX 75013-9701  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion®**  
P.O. Box 1000  
Chester, PA 19016-1000  
1-800-888-4213  
[www.transunion.com](http://www.transunion.com)

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

### **Credit Freeze**

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

**Equifax Security Freeze**  
P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Experian Security Freeze**  
P.O. Box 9554  
Allen, TX 75013-9554  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion Security Freeze**  
P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

### **Fraud Alerts**

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.



**Equifax**  
P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-766-0008  
[www.equifax.com/personal/  
credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Experian**  
P.O. Box 9554  
Allen, TX 75013-9554  
1-888-397-3742  
[www.experian.com/  
fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016-2000  
1-800-680-7289  
[www.transunion.com/fraud-  
victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Additional Information**

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

**For California Residents:** You can visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

**For Oregon Residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, Oregon 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.

**The Federal Trade Commission**  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-ID-THEFT (1-877-438-4338)  
TTY: 1-866-653-4261  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)