Our ref **1288877**

Kennedys

1600 Market Street
Suite 1410
Philadelphia, PA 19103

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267 479 6795

Nicholas.Jajko@kennedyslaw.com

November 14, 2025

Via Online Reporting

Attorney General Michael Hilgers
Consumer Affairs Response Team
2115 State Capitol
Lincoln, NE 68509

Re: **Development Services Group, Inc. – Notice of Data Event**

Dear Attorney General Hilgers:

We represent Development Services Group, Inc. ("DSG"), a research and consulting firm focused on behavioral health, justice, education, and international affairs. DSG is based in Bethesda, Maryland. We write in accordance with Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. § 87-801 *et seq.*, to report a data event resulting in the unauthorized acquisition of personal information of five (5) residents of Nebraska. This notice shall not be construed as an admission of jurisdiction or liability, nor does DSG waive its rights or defenses regarding the applicability of Nebraska law or personal jurisdiction. This notice may be supplemented with new information learned after submission.

On September 7, 2025, DSG became aware of a disruption to its computer network. DSG took immediate action to secure its systems and partnered with cyber incident professionals to investigate the nature and scope of the event. As part of the investigation, on September 22, 2025, DSG learned that data was taken from its network by an unauthorized actor. DSG commenced a detailed review of the files to understand the data potentially involved, and to whom the data belonged to. On September 28, 2025, DSG confirmed that certain files within that data set contained personal information of its current and former employees. Subsequently, DSG determined that additional review was required when it became aware that certain files concerning consultant information was also implicated. The supplemental review process was undertaken to accurately identify those additional individuals and confirm the specific data elements involved. This extended review was completed on October 29, 2025. The impacted information for all impacted individuals includes their names and Social Security numbers.

Kennedys

DSG is providing written notice of the event, via First Class U.S. mail, to the potentially impacted Nebraska residents on November 14, 2025. A sample copy of the notification letter is attached as Exhibit A

DSG's notice of this event includes a brief description of the incident, encouragement to remain vigilant for incidents of fraud or misuse, from any source, by reviewing account statements and credit reports. The notice also includes the recommendation to file a report with law enforcement, notify their state attorney general, and/or contact the Federal Trade Commission for more information. DSG confirmed the types of personal information subject to unauthorized access and enclosed contact information for the major consumer reporting bureaus, state-specific regulators, and the number for a dedicated call center for obtaining resources to protect against fraud or misuse, should the individual find it appropriate to do so. DSG is offering twelve (12) months of credit monitoring and proactive fraud assistance services through TransUnion (via CyberScout) to the impacted individuals.

Upon learning of the incident, DSG undertook immediate steps to address it, including securing its systems and taking parts of its network offline until it could safely restore operations. DSG notified federal law enforcement. It partnered with cyber incident professionals to conduct a thorough investigation and DSG reviewed its files, to confirm the population of impacted individuals and notify them as quickly as possible. DSG is also reviewing its existing security policies and protections already in place on its network for additional ways to safeguard against evolving threats. DSG is reporting to other state regulators as required.

This notice provides your Office with all information necessary to comply with Nebraska law. Please do not hesitate to contact me directly if you have additional questions.

Respectfully,

Nicholas S. Jajko

Nicholas Jajko
Partner
for Kennedys

Exhibit A

Development Services Group Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2217

0001014

5_0001014

[redacted]

November 14, 2025

Re: ***Notice of Data Breach***

Dear [redacted]:

Development Services Group Inc. ("DSG") takes the privacy and security of our employees' information seriously. As part of that commitment, we write to advise you that the data security event, which affected our computer network, potentially impacted your personal information. You are receiving this notice because you are or have worked with DSG in a consulting capacity. While we have no indications any information has been subject to actual or attempted misuse, we are providing you with the details of the event, our response, and steps you can take to help protect your personal information.

<u>What Happened?</u>

On September 7, 2025, we became aware of the disruption to our company's network. We took immediate action to secure our systems, which included taking parts of our network offline until we could safely restore operations. Upon learning of the event, we took steps to secure our systems and partnered with cybersecurity specialists to safely restore and investigate. We learned that files from our network were acquired by an unauthorized actor on September 22, 2025. We commenced a detailed review of the files to understand the data potentially involved, and to whom the data belonged. We completed the review on October 29, 2025, and we are now notifying those whose personal information was contained within the files taken.

<u>What Information Was Involved?</u>

Our review of the files confirmed your name and [redacted] were contained within certain files taken from our network. We reiterate that we have no indication of any actual or attempted fraud or misuse of your data.

<u>What We Are Doing.</u>

We notified federal law enforcement and are reviewing our existing security safeguards and we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you discover suspicious activity. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Instructions for how to enroll in these services are below.

<u>What You Can Do.</u>

We encourage you to remain vigilant for incidents of identity theft and fraud, from any source, by reviewing your credit reports and account statements for suspicious activity and errors. If you discover any suspicious or unusual activity on your accounts, promptly contact your financial institution or service provider. Please refer to the enclosed "*Steps You Can Take to Help Protect Your Information*" for the additional resources you may take advantage of to protect against fraud and identity theft, should you find it appropriate to do so.

To enroll in Credit Monitoring services at no charge, please log on to **<u>https://bfs.cyberscout.com/activate</u>** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

<u>For More Information.</u>

If you have any questions or concerns, please contact our assistance line at 1-800-405-6108, Monday through Friday, 8:00 a.m. – 8:00 p.m. Eastern time, excluding major U.S. holidays. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident.

Sincerely,

Marcia A. Cohen

President
Development Services Group, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To obtain a free annual credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Report Suspected Fraud. You have the right to file a police report if you ever experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, you will 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, your state Attorney General, and the FTC.

Place Fraud Alerts. You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Place Security Freeze. As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.)
2. Social Security number
3. Date of birth
4. Address for the prior two to five years
5. Proof of current address, such as a current utility or telephone bill
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card), and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1- 800-916-8800 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-378-4329 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Obtain Additional Information. You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the Federal Trade Commission (FTC). The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

For D.C. Residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection.

For Maryland Residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For North Carolina Residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For New Mexico Residents, you have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

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

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 4 residents of Rhode Island impacted by this incident.

Development Services Group Inc. may be contacted by mail at 7315 Wisconsin Ave., Suite 800 East, Bethesda, MD 20814. This notice has not been delayed by law enforcement.