EXHIBIT 1

By providing this notice, Lydig does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 23, 2025, Lydig discovered suspicious activity in its server environment. Lydig promptly responded and launched an investigation to confirm the nature and scope of the incident. The investigation determined that an unauthorized actor acquired certain files between June 21, 2025 and June 23, 2025. Lydig conducted a thorough review of the files acquired to confirm what was contained therein, and to whom it relates for purposes of providing notice. This review was completed on October 15, 2025.

The information that could have been subject to unauthorized access includes name, date of birth, Social Security number, driver's license number or state identification number, Passport number, financial account information, username & password, biometric information, medical information, and health insurance information.

Notice to Washington Residents

On or about December 12, 2025, Lydig provided written notice of this incident to two thousand three hundred ninety-seven (2,397) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Lydig moved quickly to investigate and respond to the incident, assess the security of Lydig systems, and identify potentially affected individuals. Further, Lydig notified federal law enforcement regarding the event. Lydig is also working to implement additional safeguards and training to its employees. Lydig is providing access to credit monitoring services for twelve (12) months through Epiq to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Lydig is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Lydig is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Lydig is providing written notice of this incident to other relevant state regulators, as necessary.

EXHIBIT A

LYDIG

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

NOTICE OF <<VARIABLE DATA 1>>

Dear <<Full Name>>:

Lydig Construction, Inc. ("Lydig") writes to make you aware of an event that may affect the security of some of your information. While we are unaware of any attempted or actual misuse of your information at this time, we are providing you with this notice in an abundance of caution, to inform you of the incident, our response, and steps you may take to help protect your information, should you feel it is necessary to do so.

What Happened? On June 23, 2025, Lydig discovered suspicious activity in our server environment. Lydig promptly responded and launched an investigation to confirm the nature and scope of the incident. The investigation determined that an unauthorized actor acquired certain files between June 21, 2025 and June 23, 2025. We conducted a thorough review of the files acquired to confirm what was contained therein, and to whom it relates for purposes of providing notice. This review was completed on October 15, 2025. We are notifying you because that investigation determined certain information related to you was contained within the impacted files.

What Information Was Involved? The review determined the following information related to you was present in the impacted files: your name and: <<Breached Elements>>.

What We Are Doing. The confidentiality, privacy, and security of personal information is among Lydig's highest priorities, and we have security measures in place to protect information in our care. Upon discovery, we promptly commenced an investigation to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying potentially impacted individuals. While we have measures in place to protect information in our care, as part of our ongoing commitment to the privacy of information, we continue to review our policies, procedures and processes related to the storage and access of personal information to reduce the likelihood of a similar future event. We will also notify applicable regulatory authorities as necessary.

As an added precaution, we are also offering <<CM Duration>> months of complimentary access to credit monitoring services through Epiq. Individuals who wish to receive these services must enroll by following the below enrollment instructions, as we are unable to enroll you in the services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious activity and to detect errors. You can review the enclosed *Steps You Can Take To Help Protect Your Personal Information* to learn helpful tips on steps you can take to protect against possible information misuse, should you feel it appropriate to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call our dedicated assistance line at 888-367-0314, Monday through Friday 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. You may also write to us at 11001 East Montgomery Drive, Spokane Valley, WA 99224.

Sincerely,

Lydig Construction, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Monitoring Services

<<Full Name>>
Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: <<CM Duration>> Months

Epiq - Privacy Solutions ID
1B Credit Monitoring - Plus

How To Enroll:

1. Visit www.privacysolutionsid.com and click "Activate Account"
2. Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3. Complete the identity verification process
4. You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5. Enter your log-in credentials
6. You will be directed to your dashboard and activation is complete!

Product Features:

1-Bureau Credit Monitoring with Alerts
Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score and Report[1]
1-Bureau VantageScore® 3.0 (annual) and 1-Bureau Credit Report.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)
Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring
Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection
Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance[2]
Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT[2]
Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Plus, please call directly at **866.675.2006,** Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

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.