EXHIBIT 1

By providing this notice, Legacy 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

In late April 2024, Legacy learned of potentially suspicious activity related to certain systems on its computer network. Legacy immediately took steps to secure its environment and investigate the nature and scope of the issue. As part of its response to this event, Legacy retained Mullen Coughlin as privacy counsel. Mullen Coughlin engaged a third-party digital forensic investigation firm on Legacy's behalf to assist with remediation of the incident and to conduct a legally privileged investigation to confirm the nature and scope of the unauthorized activity.

The third-party forensic investigation did not identify evidence that data had been taken from Legacy systems in relation to the April 2024 activity. After receiving additional information in November 2024, further investigation determined that certain files had been taken from Legacy servers by an unauthorized actor. As such, Legacy, with the assistance of third-party data review specialists, conducted a time-intensive and thorough programmatic and manual review of the impacted data set and determined that certain sensitive information was contained therein. The initial review was completed on January 31, 2025.

Legacy then undertook the vetting and retention of a third-party notification services provider to assist with the printing and mailing of notification letters, staffing of a toll-free call center to address questions from notified individuals, and the provision of complimentary credit monitoring services. The individual notification population address information compiled by Legacy was subsequently provided to the notification services provider, discussed above, and correlated with the National Change of Address database ("NCOA"). On May 1, 2025, Legacy made its final determination regarding the number of Washington residents impacted by this event.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license number, financial information, date of birth, passport number, and medical information.

Notice to Washington Residents

On or about February 28, 2025, Legacy began providing written notice of this incident to eight hundred and eighty-three (883) Washington residents. On April 9, 2025, Legacy provided written notice to three (3) Washington residents and on May 9, 2025, Legacy provided written notice to four (4) Washington residents. Written notice was 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, Legacy moved quickly to investigate and respond to the incident, assess the security of Legacy systems, and identify potentially affected individuals. Further, Legacy notified federal law enforcement regarding the event. Legacy is also working to implement

additional safeguards and training to its employees. Legacy is providing access to credit monitoring services for two (2) years through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Legacy 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. Legacy is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Legacy is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

LEGACY
PROFESSIONALS LLP
CERTIFIED PUBLIC ACCOUNTANTS

Return Mail Processing Center
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

May 9, 2025

NOTICE OF <<Variable Text 2>>

Dear <<First Name>> <<Last Name>>:

Legacy Professionals LLP ("Legacy") is a full-service accounting firm that provides professional services to individuals, corporations, not-for-profit organizations, labor unions and their related employee benefit plans. We are writing to inform you of a recent incident that may involve certain information related to you that we handle in relation to our clients. This event affected Legacy systems and did not impact any of our clients' systems. Although there is no indication that your information has been fraudulently misused in relation to this event, we are providing you with information about the event, our response to it, and steps you can take to protect your information, should you feel it appropriate to do so.

What Happened? In late April 2024, Legacy learned of potentially suspicious activity related to certain data stored on our computer network. We immediately took steps to secure our environment and investigate the nature and scope of the issue with assistance from a third-party cybersecurity specialist. After receiving additional information in November 2024, the investigation determined that certain files had been taken from Legacy servers by an unauthorized actor. Therefore, Legacy conducted a comprehensive review to identify what information was impacted and the individuals to whom the information relates. Now that the investigation is complete, we are contacting all potentially impacted individuals.

What Information Was Involved? In early February 2025, the investigation confirmed that the information on our system at the time of the incident may have included your <<Variable Text 1>>.

What We Are Doing. Legacy takes this event and the confidentiality, privacy, and security of information in our care very seriously. Upon becoming aware of this event, we immediately ensured the unauthorized access had been terminated, began investigating what happened, and reported this event to federal law enforcement. Although Legacy has always taken data security and privacy very seriously, we have implemented even more stringent access controls.

What You Can Do. We additionally encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information, 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, please contact our dedicated toll-free assistance line at 877-441-7153 Monday through Friday from 6:00 AM – 6:00 PM Pacific Time, excluding U.S. holidays; by email at notification@legacycpas.com; or by mail at P.O. Box 7008, Westchester, IL 60154.

Sincerely,

Legacy Professionals LLP

Steps You Can Take To Help Protect Personal Information

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/credit-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 Fraud Alert, 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 Credit Freeze, 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 their 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 Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.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 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.