

EXHIBIT 1

We represent Paylogix, LLC (“Paylogix”), located at 1025 Old Country Road, Westbury, New York 11590. Paylogix provides technology support for employers and insurance carriers related to employee benefits management. As such, Paylogix holds data related to individuals on behalf of its customers and partners, specifically insurers and employer groups (“Data Owners”). Paylogix is notifying your office, on behalf of the relevant Data Owners and itself, of an event that involves certain personal information relating to Washingtonians. By providing this notice, Paylogix 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 November 2025, Paylogix experienced a network disruption involving certain computer systems and services. In response, Paylogix promptly took steps to confirm the security of its systems and began a thorough investigation to determine the nature and scope of the event. The investigation confirmed that the disruption was the result of a cyber incident and that certain files may have been viewed or taken from the Paylogix network between November 13, 2025 and November 18, 2025. As a result, Paylogix undertook a comprehensive and thorough review of the relevant files to determine what information was present and to whom it related. Paylogix then worked diligently to validate and reconcile the records and identify with which Data Owners the records were affiliated. Paylogix recently completed this process and notified the Data Owners on or around July 20, 2026.

Notice to Washingtonians

On August 14, 2026, Paylogix began providing notice to individuals, including approximately twenty-eight thousand four hundred forty-nine (28,449) Washingtonians, on behalf of the relevant Data Owners and itself. The types of information associated with these Washingtonians varies by individual but may include: name, date of birth, financial account information, financial account number, health insurance information, Social Security number, and voluntary benefit information. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. While its investigation was ongoing, on January 23, 2026, Paylogix posted notice of this event to its website and on June 12, 2026, it issued notice to statewide media in all U.S. states.

Other Steps Taken and To Be Taken

In response to this event, Paylogix promptly took steps to restore the integrity of its network and ensure the security of its systems. It conducted a diligent forensic investigation to confirm the full nature and scope of the event and determine what files may be affected. It then undertook a comprehensive review effort to determine what specific information may be involved, to whom that information related, and with which Data Owner it was affiliated. Further, Paylogix recognizes the evolving nature of cybersecurity and has implemented additional technical security measures. Paylogix will continue to evaluate and enhance its security posture in the future. Paylogix also reported this event to law enforcement.

Additionally, Paylogix is providing mailed notice to individuals for whom it has contact information on behalf of the relevant Data Owners and itself. This notice includes guidance on how to better protect against identity theft and fraud, as demonstrated in the attached ***Exhibit A***. Although Paylogix is not aware of identity theft or fraud as a result of this event, this notice includes an offer of access to complimentary credit monitoring and identity theft protection services for twelve (12) months to individuals whose personal information was potentially affected by this event.

Paylogix is providing written notice of the event to certain regulatory authorities on behalf of relevant Data Owners and itself. Paylogix is also providing written notice of this event to the three (3) major credit reporting agencies: Equifax, Experian, and TransUnion.

EXHIBIT A



August 14, 2026

Dear [REDACTED]:

Paylogix, LLC (“Paylogix”) is a software as a service (“SaaS”) provider for various insurance providers. We are writing to inform you of an event that might affect some of your information. Although we are unaware of any identity theft or fraud in relation to the event, this notice provides information about what happened, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so. We likely have your information because our services were used during the enrollment process for your employee benefits at a current or former employer.

What Happened? In November 2025, Paylogix experienced a network disruption involving certain computer systems and services. In response, we promptly took steps to confirm the security of our systems and began a thorough investigation to determine the nature and scope of the event. The investigation confirmed that the disruption was the result of a cyber incident and that certain files may have been viewed or taken from the Paylogix network between November 13, 2025 and November 18, 2025. As a result, we undertook a comprehensive and thorough review of the relevant files to determine what information was present and to whom it related. We then worked to reconcile the records, identify with which of our customers the records were affiliated and notify those customers. We recently completed this process and notified the relevant customers on or around July 20, 2026. You are receiving this letter because your information was found in the relevant files.

What Information Was Involved? Based on our review, we determined that the relevant files contained your:

What We Are Doing. Our response to this event included promptly taking steps to ensure the security of our systems, conducting a diligent investigation, and undertaking a review to determine what information may be involved. We recognize the evolving nature of cybersecurity and have implemented additional technical security measures. We will continue to evaluate and enhance our security posture in the future. We also reported this event to law enforcement.

As an added precaution, we are offering you immediate access to complimentary credit monitoring and identity theft protection services for twelve (12) months through Cyberscout, a TransUnion company. You can find information on how to enroll in these services in the enclosed *STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION*. We encourage you to consider enrolling in these services as we are not able to do so on your behalf.

What You Can Do. We 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. You can review the enclosed *STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION* to learn helpful tips on steps you can take to protect against possible information misuse, should you feel it appropriate to do so. You may also enroll in the complimentary monitoring services that we are offering to you.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at [REDACTED] from 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Paylogix, LLC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you on the same day that the change or update takes place with the bureau.

In order for you to receive the monitoring services described above, you must enroll within ninety (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 eighteen (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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus: Equifax, Experian, and TransUnion. To order a free credit report, visit <https://www.annualcreditreport.com> or call, toll-free, 1 (877) 322-8228. Consumers may also directly contact the three (3) 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 one (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 (7) years. Should consumers wish to place a fraud alert, please contact any of the three (3) 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 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 (2) to five (5) 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 (3) 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 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; <https://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, the relevant state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and <https://oag.dc.gov>. Paylogix is located at 1025 Old Country Road, Suite 310, Westbury, New York 11590.

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://oag.maryland.gov>. Paylogix is located at 1025 Old Country Road, Suite 310, Westbury, New York 11590 and its website may be found at <https://www.paylogix.com>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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 <https://www.ncdoj.gov>.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; <https://www.riag.ri.gov>; and 1 (401) 274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 634 Rhode Island residents that may be impacted by this event.