EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Colaberry does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 6, 2026, Colaberry learned that a file containing Form W-2s for 2025 employees had been inadvertently sent to an unauthorized actor in response to a spoofed phishing email. In response, Colaberry promptly launched an investigation into the nature and scope of the event and notified the IRS of what happened.

The information involved includes name, Social Security number, and other information contained in current and former employee's 2025 Form W-2 issued by Colaberry.

Notice to Maine Resident

On March 24, 2026, Colaberry provided written notice of this event to individuals including one (1) Maine resident. 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 learning of the event, Colaberry moved quickly to investigate the event, notify the IRS of what happened so they can monitor against fraudulent tax filing activity, and undertake a review to determine what information may be involved. Colaberry is working to implement additional safeguards and training for its employees to protect against similar events in the future. Colaberry is also providing access to complimentary credit monitoring and identity theft protection services for twenty-four (24) months, through Cyberscout, a TransUnion company, to individuals.

Additionally, Colaberry is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including encouraging individuals to file their 2025 tax returns as soon as possible, if not done so already. Colaberry 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. Colaberry is providing written notice of this event to relevant state privacy regulators and to the three (3) major credit reporting agencies: Equifax, Experian, and TransUnion.

EXHIBIT A

Colaberry, Inc.
c/o Cyberscout
PO Box 245
Bellmawr, NJ 08099

Colaberry

USBFS3145 - T1 P1 - 41

[redacted]

0102000041

March 24, 2026

Dear [redacted]:

As part of Colaberry Inc. ("Colaberry")'s commitment to your privacy and security, we are writing to provide you notice of a recent event involving information contained on your 2025 Form W-2. This letter 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.

What Happened? On February 6, 2026, Colaberry learned that a file containing Form W-2s for 2025 employees had been inadvertently sent to an unauthorized actor in response to a spoofed phishing email. In response, we promptly launched an investigation into the nature and scope of the event and notified the IRS of what happened.

What Information Was Involved? Colaberry is notifying you now because the following types of information related to you were involved in this event: name, Social Security number, and other information contained on your 2025 Form W-2 issued by Colaberry.

What We Are Doing. Information privacy and security are among Colaberry's highest priorities. Our response included completing an investigation, notifying the IRS of what happened so they can monitor against fraudulent tax filing activity, and undertaking a review to determine what information may be involved. We are reviewing existing security policies and have reinforced with our staff the importance of safeguarding information in our possession to protect against similar events moving forward.

As an added precaution, we are offering you immediate access to complimentary credit monitoring and identity theft protection services for twenty-four (24) 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 file your 2025 tax return and/or consult with your tax filing professional regarding this issue as soon as possible, if you have not done so already. We also 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. Additionally, 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 credit monitoring services we are offering to you.

000041002001

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 call [redacted] from 8:00 a.m. ET to 8:00 p.m. ET, Monday through Friday, excluding major U.S. holidays.

Sincerely,



Angela D. Mezo
Director of HR & Immigration
Colaberry, Inc.

0102000041

0000410020101

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]

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.

File Your 2025 Tax Return. We encourage you to file your 2025 tax return as soon as possible, if you have not already done so. You can visit the IRS's website at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. If you become aware of a fraudulent tax return filed in your name or you are instructed to do so by the IRS, you should file the IRS Form 14039, Identity Theft Affidavit, with a paper copy of the return, and mail according to the instructions. A copy of this form can be found at https://www.irs.gov/pub/irs-pdf/f14039.pdf or https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. You should also look at the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit https://www.taxadmin.org/state-tax-agencies.

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 http://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.

0202000041

0000410020202

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. Colaberry is located at 100 Summit Drive, Burlington, Massachusetts 01803.

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 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.

0202000041

0000410020202