Bridgewell

[redacted]

[redacted]

[redacted]

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to us. We are writing to provide you with important information about a recent data security incident which involves some of your personal information. As such, we wanted to provide you with information about the incident, explain the services that we are making available to you, and precautionary measures you can take to protect your information.

On or about April 6, 2026, we detected unauthorized access to our iSolved platform as a result of a cybersecurity incident. Upon learning of this issue, we commenced a prompt and thorough investigation assisted by cybersecurity professionals experienced in handling these types of incidents. At the completion of our investigation on June 15, 2026, we determined that your account may have been subject to unauthorized access and certain personal information may have been viewed on April 6, 2026. The potentially impacted information includes your [redacted]

We want to make you aware of the incident and provide you with complimentary access to identity theft protection services through IDX as a precaution. IDX identity protection services include [redacted] months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your information is compromised. This is completely free to you and enrolling in this program will not hurt your credit score.

We encourage you to contact IDX with any questions and to enroll in the services by calling [redacted], going to [redacted] and using the following Enrollment Code. [redacted]. Enrollment Code: [redacted]

This letter also provides more information about the complimentary services and other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

We remain fully committed to maintaining the privacy of personal information entrusted to our care. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. If you have any further questions regarding this incident, please call [redacted]

[redacted] at [redacted]. We have taken this matter very seriously and apologize for any inconvenience or concern this may cause.

Sincerely,

Bridgewell, Inc.
10 Dearborn Road
Peabody, MA 01960

– OTHER IMPORTANT INFORMATION –

1. Complimentary Identity Protection Services.

To enroll in the complimentary services, call IDX at [redacted] or go to [redacted] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. IDX representatives are available Monday through Friday from [redacted] am - [redacted] pm Eastern Time. Please note the deadline to enroll is [redacted]. The identity protection services through IDX include all of the following:

- **SINGLE BUREAU CREDIT MONITORING:** Monitoring of credit bureau for changes to the member's credit file such as new credit inquiries, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- **CYBERSCAN™:** Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.
- **IDENTITY THEFT INSURANCE**: Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.
- **FULLY-MANAGED IDENTITY RECOVERY:** ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

We encourage you to contact IDX with any questions about the identity protection services by calling [redacted]. IDX representatives are available Monday through Friday from [redacted] a.m. to [redacted] p.m. Eastern Time.

2. Placing a Fraud Alert.

We recommend that you place a one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to take reasonable steps to verify your identity before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. Once one credit bureau confirms your fraud alert, it is required to notify the others.

Equifax	***Experian***	***TransUnion***
Equifax Information Services LLC P.O. Box 105069, Atlanta, GA 30348 www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ 1-888-EQUIFAX (1-888-378-4329)	P.O. Box 9532, Allen, TX 75013 www.experian.com/fraud 1-888-EXPERIAN (1-888-397-3742)	Fraud Victim Assistance Department P.O. Box 2000, Chester, PA 19016 www.transunion.com/fraud-alerts 800-916-8800; 800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

You may also request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting any of the three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
Equifax Information Services LLC
P.O. Box 105788, Atlanta, GA 30348
www.equifax.com/personal/credit-report-services/credit-freeze/
1-888-EQUIFAX (1-888-378-4329)

Experian Security Freeze
P.O. Box 9554, Allen, TX 75013
www.experian.com/freeze
1-888-EXPERIAN (1-888-397-3742)

TransUnion Security Freeze
P.O. Box 160, Woodlyn, PA 19094
www.transunion.com/credit-freeze
800-916-8800; 888-909-8872

To place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as a copy of a government-issued identification. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. If you do place a security freeze prior to enrolling in identity theft protection services, you will need to remove the freeze to sign up. After you sign up, you may refreeze your credit file.

4. Obtaining a Free Credit Report.
Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies, identify any accounts you did not open or inquiries from creditors that you did not authorize, and verify that all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Protecting Medical Information.
As a general matter, the following practices can help deter, detect, and protect against medical identity theft. For more information, visit consumer.ftc.gov/articles/what-know-about-medical-identity-theft. Only share health insurance cards with health care providers and family members who are covered under the insurance plan or who help with medical care. Review the “explanation of benefits" statement provided by the health insurance company and follow up with the insurance company or care provider regarding any unrecognized items. If necessary, contact the care provider listed on the explanation of benefits statement and request copies of medical records from the date of potential access (noted above) through the current date. Ask the insurance company for a current year-to-date report of all services paid for the impacted individual as a beneficiary and follow up on any unrecognized charges.

6. Additional Helpful Resources.
Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by visiting www.identitytheft.gov, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.