Exhibit A

Please read this message in its entirety.

Reframe

Via Email

June 30, 2026

Re: Notice of Data Breach

Dear Reframe User:

We're writing to let you know about a security incident that involved some information from your Reframe account. The trust you place in us is something we take seriously, and as part of our commitment to you, we're providing this notice to explain what happened, what information may have been involved, what we are doing, and what steps you can take to protect yourself online.

WHAT HAPPENED

Reframe recently discovered that a single system was accessed without authorization. We acted quickly to stop the activity and engaged cybersecurity experts to assist with an investigation. While we were able to confirm the limited scope of the issue, our investigation found that, before we addressed it, some of your personal information uploaded to Reframe was downloaded without authorization on or around May 1, 2026.

WHAT INFORMATION WAS INVOLVED

Your personal information involved was [redacted].

The incident did not include your Reframe password, and it did not include your home or mailing address, any payment card or payment account information or any other financial information. Reframe payments are handled through separate systems that were not affected. We do not collect Social Security numbers, driver's license numbers, or other government identifiers, so none were involved.

We also have no indication that any of the information involved in this incident has been misused.

WHAT WE ARE DOING

This incident did not involve your Social Security number, payment information, mailing address, or any financial information. However, to give you added peace of mind, we are offering you 12 months of

complimentary credit monitoring and dark web monitoring services through TransUnion, at no cost to you. Details on how to enroll are included below the signature line.

We understand that what you share with Reframe is your journey and protecting that trust is something we take to heart. In addition to the comprehensive security measures our company had in place prior to the incident, we have taken steps to further enhance the security of our systems, including enhancing our security and monitoring controls. We will continue to advance our IT security and data privacy controls to stay ahead of an ever-evolving threat landscape.

WHAT YOU CAN DO

It is always a good idea to be cautious of unsolicited communications—whether by email, text message, or phone—that reference your health, wellness, or personal habits. These communications could be phishing or social-engineering attempts. Do not click links or provide additional personal information in response to suspicious messages.

As an added measure, we encourage you to take advantage of the complimentary credit monitoring and dark web monitoring we are providing through TransUnion, at no cost to you. You can enroll using the instructions provided below the signature line. We also encourage you to wish to review your account statements periodically as a general precaution and to review the additional information about identity protection below the signature line.

For More Information

We have established a dedicated call center to answer questions about the security incident. If you have any questions, please call the call center at 1-844-593-7750, from 8 a.m. to 8 p.m. ET Monday through Friday, excluding major U.S. holidays.

We deeply regret that this security incident occurred, and we remain committed to protecting the information users entrust to us.

Sincerely,

Reframe Support Team
Glucobit, Inc. d/b/a Reframe
6120 Windward Pkwy, #165
Alpharetta, GA 30005

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH TRANSUNION CREDIT MONITORING SERVICES

To activate your membership and start monitoring your personal information, please follow the steps below:

For Adults:

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. 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 the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by CyberScout, a TransUnion company specializing in fraud assistance and remediation 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 to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and email account and may not be available to minors under the age of 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.

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. customers are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free +1 (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR A SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or a security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	Experian	TransUnion
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
(800) 525-6285	(888) 397-3742	(877) 322-8228
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five (5) years;
5. Proof of current address such as a current utility bill or a telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission (FTC) for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357 or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state Attorney General, or the FTC.

California residents: Visit the California Office of Privacy Protection https://oag.ca.gov/privacy for additional information on protection against identity theft.

New York residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224 0341; +1 (800) 771-7755 or www.ag.ny.gov.

Oregon residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

For California, Montana, and Washington: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).