Bidra Innovation Ventures
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

[redacted]

October 2, 2026

NOTICE OF DATA BREACH

Dear [redacted],

Bidra Innovation Ventures is writing to inform you of a data-security incident on one of our vendors' servers that affected some of your information. We are providing this notice to explain what happened, what we are doing in response, and how you can enroll in our offer of free credit monitoring and identity-theft-protection services.

WHAT HAPPENED

On June 10, 2025, our vendor, Kranz Consulting, suffered a cybersecurity incident involving unauthorized access to systems containing Bidra data. The affected systems were fully maintained by Kranz, making Bidra reliant on Kranz's forensic investigation to identify the potentially impacted dataset. Following completion of the investigation, Kranz provided the affected files to Bidra, after which we engaged an independent data review firm to determine whether personal information was involved and identify impacted individuals. Bidra received the results of that review on April 14, 2026, and has since been developing a notification process and gathering the contact information necessary to provide the notice you received today.

WHAT INFORMATION WAS INVOLVED

We determined that the following types of information related to you were contained in the affected systems: [redacted].

WHAT WE ARE DOING

We worked with Kranz to facilitate the removal of Bidra data from Kranz's systems. Kranz also informed us that it implemented additional security measures, including additional endpoint detection and response tools.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance included in this letter. In addition, we are offering you [redacted] months of complimentary credit monitoring services provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. This product helps detect possible misuse of personal information. To enroll in credit monitoring, please:

- Visit and log on to https://bfs.cyberscout.com/activate and follow the instructions provided
- When prompted, provide your **unique code:** [redacted]

In order for you 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 e-mail 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. If you have questions or want an alternative to enrolling in Cyberscout, please email customer.support@cyberscout.com.

FOR MORE INFORMATION

We have established a toll-free call center to support you and answer your questions. You can contact the call center at 1-800-405-6108, and one of our representatives will be happy to assist you. We appreciate your patience as we work through this process.

Sincerely,

Bidra Innovation Ventures

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/.

You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.

You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your credit report, free of charge, once per week. We recommend you do so and if the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

- **Equifax**. PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian**. PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion**. PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You should also consider contacting the Federal Trade Commission for more details on protecting yourself from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. A fraud alert is free and will stay on your credit report for one (1) year, but you can renew it. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.

A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov/ to report the issue and get recovery steps.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect yourself from fraud or identity theft. You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

New York Residents. You can contact the New York Attorney General at The Capitol, Albany, NY 1224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.

North Carolina Residents. You can contact the North Carolina Attorney General at 90001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6400 or visit their website, www.ncdog.gov.

Washington, DC Residents. You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.