Dear Investor, 30733

We are writing to inform you of a recent security incident that may have impacted your personal information or the confidential information of the institutional investor with which you are associated. This incident did not occur within North Island Venture's network or systems and instead occurred at our third-party administrator, as described below.

What happened?

We recently learned from MG Stover & Co ("MG Stover") that, on or around September 19, 2023, an unauthorized party gained access to MG Stover's account in the Retool application and gained access to certain fund data, including the information we have shared with MG Stover. We are providing this notice in an abundance of caution and to enable you to take steps to help protect your information.

North Island Ventures engages MG Stover to provide fund administration services, including portfolio processing and reconciliation, tax preparation, and distribution support. In connection with those services, we provide MG Stover with certain investor information. MG Stover utilizes a third-party developer, Retool, to develop internal business applications and regulate data from fund accounting applications in the provision of services to North Island Ventures.

What Information Was Involved?

MG Stover advised that the unauthorized party was able to query data from the systems connected to Retool, which contained certain data about our individual investors and institutional investors and their representatives. The types of information included will depend on the applicable investment fund. Based on the information provided by MG Stover, the following information may have been accessible:

- **North Island Ventures Fund I LP and NIV Fund II LP -** Names of investor, mailing addresses, investor commitments, contributions, and capital details.

- **NIV Voyager Fund –** Names of investor, email address, phone number, mailing address, date of birth, Social Security numbers or Taxpayer Identification Numbers, and names and email addresses of interested party(ies).

What We Are Doing

While this incident did not occur at North Island Ventures, we are committed to the protection of your information and providing investors with available information regarding this matter so you can take action to protect your information. MG Stover also represented to us that they successfully contained the incident and terminated all unauthorized access. MG Stover has also advised that they are taking steps to help prevent a similar occurrence in the future.

What You Can Do

We encourage you to review the enclosed additional information and actions that you can consider taking to help protect your information.

More Information

If you have questions or concerns, please contact Charles Moran at charles@northisland.ventures or Shivank Kumar at shivank@northisland.ventures.

ADDITIONAL RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

The Federal Trade Commission

600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Credit Reporting Agencies

Equifax	**Experian**	**TransUnion**
PO Box 740241	PO Box 4500	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditregort.com. by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When

you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For District of Columbia Residents: You may also obtain information about preventing and avoiding identity theft from the District of Columbia Office of the Attorney General:

District of Columbia Office of the
Attorney General
Office of Consumer Protection
400 6th Street, NW, Washington, DC
20001 (202) 442-9828
www.oag.dc.gov

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney
General Consumer Protection
Division
200 St. Paul Place, Baltimore, MD
21202 1-888-743-0023
www.oag.state.md.us

For Massachusetts Residents: You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub, or statement) in order to implement your request for a security

freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office:

New York Attorney General's Office
Bureau of Consumer Frauds & Protection
The Capitol, Albany, NY 12224
1-800-771-7755
www.ag.ny.gov

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center Raleigh,
NC 27699-9001
1-877-5-NO-SCAM
www.ncdoi.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street Providence, RI 02903
1-401-274-4400
riag.ri.gov

Dear Investor,

You recently received a message from our team regarding a security incident that occurred at our third-party administrator, MG Stover & Co.

To comply with our obligations under certain U.S. state laws, we are offering – at no charge to you – two years of credit monitoring and identity theft services through Experian's® IdentityWorksSM. Below we have provided instructions on how to enroll in these services.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is <u>immediately available to you</u>, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** January 31, 2024. Enrollments must occur by no later than 5:59 P.M. CT. (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: http://www.experianidworks.com/credit
- Provide your **activation code**: [redacted]

If you have questions about these serivces, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by January 31, 2024. Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you have questions regarding the Experian services or how to enroll, please contact Experian's customer care team at 1-877-890-9332. If you have additional questions or concerns please contact Shivank Kumar, General Counsel, at North Island Ventures at shivank@northisland.ventures.

Sincerely,

[CONTACT]
North Island Ventures

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.