EXHIBIT 1

EMAIL SUBJECT: Notice of Vendor Data Incident

Dear Investor,

We value our partnership and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident affecting one of our service providers, Kranz Consulting ("Kranz"), that may involve your personal information. Kranz, a third party fund administrator to the industry, recently reported to us that on or about June 10, 2025, it noticed some suspicious activity on one of its networks. See their letter to us in Attachment 1, which contains details of what happened, and what they have done to address the issue. In the interest of caution, we are assuming that all data contained in the Subscription Agreement you signed with us, such as contact details (including name, email address, mailing address), identifiers such as social security number of individuals or EIN of entities, and banking details (such as wire transfer instructions and bank account numbers) were potentially impacted at some point. Less than seventy-five (75) of our individual LPs' data appear to be potentially affected.

While Kranz has indicated they took all necessary measures to ensure the security of the impacted dataset and has represented it was able to keep any potentially exfiltrated data protected, safe, and secure, we still suggest monitoring your data. Please review Attachment 2 to this letter (Steps You Can Take to Further Protect Your Information).

For further information please contact: Greg Stupore, CFO of Silas, at greg@silascapital.com (phone (631) 871-0733) and we will coordinate obtaining answers to your questions with Kranz.

Sincerely,

Carter Weiss, Frank Lin, Brian Thorne

Silas Capital | 1330 Sixth Ave, Fl 14, NY, NY 10019

Kranz Consulting
655 Montgomery St, 12th Floor
San Francisco, CA 94111

July 31, 2025

RE: Kranz Consulting Update

Dear Greg and Carter,

Kranz Consulting became aware of suspicious activity on certain servers in its computer network on June 10, 2025. Following our initial discovery of suspicious activity in our environment, we immediately shut down our network. We also promptly engaged our insurance provider, legal counsel, third-party forensic specialists, and a restoration vendor to start an investigation into the incident. We then worked to restore our systems as quickly and safely as possible.

To ensure the continued security of our systems, our forensic team deployed an Endpoint Detection and Response (EDR) tool to all available endpoints on the Kranz Consulting and broader Addison Group networks, along with a new MDR, ZeroTrust VPN, and other tools. Next, we created a new AWS environment, firewall, and servers while confirming that each individual endpoint and user account was confirmed to not be impacted. All users were then reentered into the Kranz Consulting environment with new, highly secure passwords. We are confident that our already robust security posture and the additional steps taken in response to this event will mitigate the chance of something like this happening again.

After completing our thorough investigation, we determined that an unknown dataset was exfiltrated from our environment. We immediately took all the necessary measures recommended by our insurance provider, legal counsel, and forensic specialists to ensure the security of the impacted dataset. Those measures included paying a ransom and receiving confirmation from our third-party forensic investigators that the entire impacted dataset was destroyed. Therefore, we were able to keep any potentially exfiltrated data protected, safe, and secure. We also are not anticipating any other business impact to our clients or their partners. Our IT team will continue to monitor specific avenues where data is illegally sold for a minimum of 12 months to confirm if any data was compromised and released. If we determine that any data has been released, we will contact you at that time. We have also taken the additional step of changing passwords to all client-related systems out of an abundance of caution. **At this time, we are effectively considering all matters related to the security incident closed**.

As part of our ongoing commitment to safeguarding the privacy and safety of information provided to us, we have also implemented enhanced internal data security systems, including advanced security software on all Kranz Consulting devices.

Please know that client safety, trust, and transparency are always of the utmost importance to us. If you have any questions or concerns, please get in touch with your Kranz Consulting representative at any time.

Thank you for being a valued client. We are excited to move forward and continue our esteemed partnership with you.

Sincerely,

Manuel Azuara
President

Attachment 2

Steps You Can Take to Further Protect Your Information

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the printable request form at https://www.annualcreditreport.com/manualRequestForm.action or fill out the online form at https://www.annualcreditreport.com/requestReport/requestForm.action. You may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

	Equifax	**Experian**	**TransUnion**
Contact Information	(866) 349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	(888) 397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	(800) 888-4213 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://consumer.ftc.gov/identity-theft-and-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

- **Contacting Your State Attorney General**

California residents may request additional information by contacting the California Office of the Attorney General at the below address, or by calling (800) 952-5225, or by visiting https://oag.ca.gov/idtheft.

California Office of Attorney General
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550

Connecticut residents may request additional information by contacting the Connecticut Office of the Attorney General at the below address, or by calling 860-713-6300 or 800-842-2649 (toll free), or by visiting https://portal.ct.gov/ag/consumer-issues/identity-theft/identity-theft.

Connecticut Office of Attorney General
165 Capitol Avenue
Hartford, CT 06106

Florida residents may request additional information by contacting the Florida Office of the Attorney General at the below address, or by calling 1-866-966-7226 (toll free), or by visiting https://www.myfloridalegal.com/identity-theft/preventing-identity-theft.

Florida Office of Attorney General
PL-01, The Capitol
Tallahassee, FL 32399-1050

Massachusetts residents may request additional information by contacting the Massachusetts Office of the Attorney General at the below address, or by calling 617-973-8787, or by visiting https://www.mass.gov/info-details/identity-theft. Massachusetts residents also have the right to obtain a police report regarding the incident by contacting their local police department. The attorney general's office information is below.

Massachusetts Office of Attorney General
1 Federal Street
Suite 0720
Boston, MA 02110-2012

Missouri residents may request additional information by contacting the Missouri Office of the Attorney General at the below address, or by calling 573-751-3321, or by visiting https://ago.mo.gov/get-help/programs-services-from-a-z/identity-theft-data-security/.

Missouri Office of Attorney General
Supreme Court Building
207 W. High St.
P.O. Box 899
Jefferson City, MO 65102

New Jersey residents may request additional information by contacting the New Jersey Office of the Attorney General at the below address, or by calling 609-292-4925, or by visiting https://www.njoag.gov/new-jersey-division-of-consumer-affairs-new-jerseyans-affected-by-recent-data-breaches-can-take-basic-steps-to-protect-against-identity-theft/.

New Jersey Office of Attorney General
Richard J. Hughes Justice Complex (HJC)
8th Floor, West Wing
25 Market Street
Trenton, NJ 08625-0080

New York residents may request additional information by contacting the New York Office of the Attorney General at the below address, or calling 1-800-771-7755, or visiting https://ag.ny.gov/publications/identity-theft.

New York Office of Attorney General
The Capitol
Albany, NY 12224-0341

North Carolina residents may request additional information by contacting the North Carolina Office of the Attorney General at the below address, or calling 877-566-7226 (Toll-free within North Carolina) or 919-716-6000, or by visiting https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

North Carolina Office of Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001

Ohio residents may request additional information by contacting the Ohio Office of the Attorney General at the below address, or calling 800-282-0515 (toll-free), or visiting https://www.ohioattorneygeneral.gov/Individuals-and-Families/Consumers/Identity-Theft.

Ohio Office of Attorney General
30 E. Broad St., 14th Floor
Columbus, OH 43215

Pennsylvania residents may request additional information by contacting the Pennsylvania Office of the Attorney General at the below address, or calling 717-787-3391, or visiting https://www.attorneygeneral.gov/wp-content/uploads/2025/03/ID_Theft.pdf.

Pennsylvania Office of Attorney General
Strawberry Square
Harrisburg, PA 17120

Virginia residents may request additional information by contacting the Virginia Office of the Attorney General at the below address, or calling 804-200-4215, or visiting https://www.oag.state.va.us/programs-outreach/identity-theft.

Virginia Office of Attorney General
202 North Ninth Street
Richmond, VA 23219

- Security Freeze

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.