Date: August 16, 2023

[Insert recipient name]
[Insert recipient's address]

NOTICE OF DATA BREACH

Dear XXXXXX,

We are writing to you because of an incident involving potential access to your personal information associated with our e-mail system (the "Incident"). This Notice is sent pursuant to the New York State Information and Security Breach and Notification Act, amended by the New York SHIELD Act (General Business Law Section 899-aa).

While we have seen no indication of misuse of information to date, we are providing notice to you and other potentially affected individuals about the Incident and encourage you to closely monitor the information that we describe below (see **What Personal Information Was Involved?**). You can use the tools we share below to protect yourself against possible unauthorized use of information such as identity theft or fraud.

What Happened?

Between July 31, 2023 and August 9, 2023, an unknown and unauthorized actor (the "Hacker") gained unauthorized access to the e-mail account of a Mansueto Ventures employee. As a result of that unauthorized access, the Hacker would have been able to view information in the Mansueto Ventures employee's e-mail. The Mansueto Ventures employee's e-mail contained what could be your personal financial information. At this time, Mansueto Ventures has no indication of misuse of your potential personal information.

What Personal Information Was Involved?

The potential personal information included in the Mansueto Ventures employee's e-mail accessed by the Hacker included the following:

- Your contact information, including your name, e-mail, address, phone number; and
- Potentially, your financial information, including bank account number and bank routing number. Our records do not indicate whether the financial information was your personal financial information or the financial information of your employer.

What We Are Doing

We take privacy and security of data seriously. Mansueto Ventures has reported the Incident to the U.S. Federal Bureau of Investigation ("FBI") and is not aware of on-going investigation in the Incident by the FBI at this time. Therefore, there is no delay in this Notice due to any pending investigation.

The cybersecurity firm engaged by Mansueto Ventures is investigating Mansueto Ventures' systems, including information and communications systems.

Again, although there is no evidence that your potential personal information has been fraudulently used, Mansueto Ventures is offering enrollment in one year (12 months) of complimentary LifeLock Ultimate Plus Identity Theft Protection services.

What You Can Do

Despite no indication that your personal information has been misused by the Hacker, you should monitor the accounts associated with the personal information provided to Mansueto Ventures for any unauthorized activity. We also suggest that you promptly contact the financial institutions associated with the personal information, and request that they monitor your accounts for any unauthorized activity.

We also encourage you to remain vigilant against threats of identity theft or fraud, and to regularly review your credit card statements and credit reports for any unauthorized activity with your personal information. It is also good practice to change all your log-in and account information, including those associated with the personal information that was provided to Mansueto Ventures, in light of this notice and on a regular basis, and never use the same password for multiple system logins.

You can also enroll in one year (12 months) of complimentary LifeLock Ultimate Plus Identity Theft Protection, upon request. In order to request this service, please contact Mark Rosenberg, Mansueto Ventures' CFO, at (212) 389 5223.

You can also follow the recommendations included in this letter, including those in the "**Steps You Can Take to Further Protect Your Information**" section below, which includes resources and information about how to protect your personal information.

For More Information.

If you have any questions about this letter, please call Mark Rosenberg, Mansueto Ventures' CFO, from 9:00 a.m. to 5:00 p.m. Eastern Time at (212) 389 5223 or write to me at:

Mark Rosenberg
Mansueto Ventures
7 World Trade Center 29th Floor
New York, NY 10007-2195

We appreciate your patience and understanding on this matter.

Very Truly Yours,

Mark Rosenberg
CFO

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, your state attorney general, and/or the Federal Trade Commission ("FTC").

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Credit Reports: Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. You are also entitled to a free credit report once every 12 months from each of these agencies at www.annualcreditreport.com, call toll-free 877-322-8228 or by completing an Annual Credit Request Form at www.ftc.gov/bcp/menus/consumer/credit/rights.shtm and mailing to:

Annual Credit Report Request Service,
P.O. Box 1025281
Atlanta, GA 30348-5283.

You can also obtain a credit report by contacting one of the following three national credit reporting agencies by phone (toll-free) and online:

Equifax: equifax.com/personal/credit-report-services or 1-800-685-111	Experian: experian.com/help or 1-888-397-3742	TransUnion: transunion.com/credit-help or 1-888-909-8872

When you receive your credit reports, review your credit reports for accounts and inquiries you don't recognize, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. These can be signs of identity theft. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report.

You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the U.S. Federal Trade Commission ("FTC") at the FTC address, phone number or website listed for the FTC above in the "**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**" section.

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

Fraud Alerts: The FTC recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus using the contact information below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert is free and stays

on your credit report for one year. You can renew it after one year. Additional information is available at http://www.annualcreditreport.com.

Equifax	Experian	TransUnion
https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf	https://www.experian.com/fraud/center.html	https://www.transunion.com/fraud-alerts

Credit Freeze: You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a freeze, contact each of the major credit bureaus using the information below. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-800-349-9960	1-888-397-3742	1-800-909-8872
https://www.equifax.com/personal/credit-report-services/credit-freeze/	https://www.experian.com/freeze/center.html	https://www.transunion.com/credit-freeze

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, provide the addresses where you have lived over the prior five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) business day after receiving a telephone or secure electronic request, or three (3) business days after receiving your written request, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security

freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you place the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

For Massachusetts residents: Under Massachusetts law, you have the right to obtain any police report filed 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. There is no fee for you to request, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.