

21918



ADVANCED TECHNOLOGY VENTURES

BOSTON MENLO PARK ::
500 Boylston Street, Suite 1380, Boston, MA 02116
617.933.3770 www.atvcapital.com

August [], 2021

[Name]
[Address]
[City], [State] [ZIP]

NOTICE OF DATA BREACH

Dear [Name],

We are writing to inform you of an information security incident that involves certain personal information you provided to Advanced Technology Ventures ("ATV" or the "Company"). We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened?

On July 9, 2021 the Company learned from its third-party information technology provider that there had been anomalous activity on two identical ATV servers (the "Servers") on which the Company stored financial reporting information. The Company soon determined that the Servers had been encrypted by a ransomware attack. On July 26, 2021, the Company learned that there was evidence of both unauthorized access to and exfiltration of the contents of the Servers.

What Information Was Involved?

Although the Company has not yet confirmed the precise categories of personal information that were accessed on a per-individual basis, the Company has reason to believe it included the names, email addresses, phone numbers, and Social Security Numbers of individual investors in the Company's funds. We are not at this time aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

We take the privacy of personal information seriously and deeply regret the occurrence of this incident. We took steps to address this incident promptly after it was discovered. We notified the FBI, launched an internal investigation and retained a forensic investigation firm to assist in the investigation of and response to this incident. We also required all employees to change their access credentials and deployed additional endpoint protection on our corporate network to help prevent this type of incident from reoccurring in the future.

We are providing two years of free identity theft protection and credit monitoring services from a leading identity monitoring services company for individuals who opt in. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the enrollment instructions included with this letter.

What You Can Do

Although we are not aware of fraud arising from this incident, we want to make you aware of precautionary steps you can take:

- **Activating the Complimentary Identity Protection Services.** As outlined above, we are offering two years of free identity theft protection and credit monitoring services. For more information about these services and instructions on completing the enrollment process, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter. Note that you must complete the enrollment process by [DATE].
- **Checking Credit Reports and Financial Accounts.** You should carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed on the next page.

If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. You can also inform your state attorney general's office and the Federal Trade Commission ("FTC"). You can review your financial account statements to determine if there are any discrepancies or unusual activity. If you see discrepancies or unusual activity on



ADVANCED TECHNOLOGY VENTURES

BOSTON MENLO PARK ::
500 Boylston Street, Suite 1380, Boston, MA 02116
617.933.3770 www.atvcapital.com

your financial account statements, or see anything you do not understand, call the financial institution immediately.

- **Consulting the Identity Theft Protection Guide.** Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact us at 650-352-6650 between the hours of 9 AM to 5 PM Pacific time, Monday through Friday or via email at MCarusi@atvcapital.com. Again, we sincerely regret any concern this incident may cause.

Sincerely,

Mike Carusi
Managing Director

Information about Identity Theft Protection

To help protect your identity, we are offering complimentary access to Experian's® IdentityWorksSM for two years.

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 at **[NUMBER]**. 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 this Identity Restoration support is available to you for **[TIMEFRAME]** 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 immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary two year membership.

This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: [DATE]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **[LINK]**
- Provide your **activation code: [CODE]**

Additional Details Regarding Your Two-Year 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.¹
- **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.
- **Up to \$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² 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.

obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should 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 Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For additional information from the IRS about identity theft, please visit <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft> or call 800-908-4490. There may be similar resources available at the state level, and you can contact your state department of revenue directly for more information. A listing of state tax agencies' websites is available at <http://www.taxadmin.org/state-tax-agencies>.

For residents of Maryland: 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 residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/internet/privacy-and-identity-theft>.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from 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.ncdoj.gov.

For residents of the District of Columbia: You may also obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia: Office of the Attorney General for the District of Columbia, Office of Consumer Protection, 400 6th Street NW, Washington, D.C. 20001 202-442-9828, www.oag.dc.gov.

Security Freezes and Fraud Alerts: You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

For more information, including information about additional rights, you can visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>, <https://www.consumerfinance.gov/learnmore/>, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)	Experian (www.experian.com)	TransUnion
General Contact:	General Contact:	(www.transunion.com)
P.O. Box 740241, Atlanta, GA 30374	P.O. Box 2104, Allen, TX	General Contact, Fraud Alerts
800-685-1111	75013	and Security Freezes:
Fraud Alerts and Security Freezes:	888-397-3742	P.O. Box 2000, Chester, PA
P.O. Box 740256, Atlanta, GA 30374	Fraud Alerts and Security	19022
	Freezes:	800-916-8800
	P.O. Box 9556, Allen, TX	
	75013	



August [], 2021

[Name]
[Address]
[City], [State] [ZIP]

NOTICE OF DATA BREACH

Dear [Name],

We are writing to inform you of an information security incident that involves certain personal information you provided to Lightstone Ventures ("Lightstone" or the "Company"). We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened?

On July 9, 2021 the Company learned from its third-party information technology provider that there had been anomalous activity on two identical Lightstone servers (the "Servers") on which the Company stored financial reporting information. The Company soon determined that the Servers had been encrypted by a ransomware attack. On July 26, 2021, the Company learned that there was evidence of both unauthorized access to and exfiltration of the contents of the Servers.

What Information Was Involved?

Although the Company has not yet confirmed the precise categories of personal information that were accessed on a per-individual basis, the Company has reason to believe it included the names, email addresses, phone numbers, and Social Security Numbers of individual investors in the Company's funds. We are not at this time aware of any fraud or misuse of your information as a result of this incident.



What We Are Doing

We take the privacy of personal information seriously and deeply regret the occurrence of this incident. We took steps to address this incident promptly after it was discovered. We notified the FBI, launched an internal investigation and retained a forensic investigation firm to assist in the investigation of and response to this incident. We also required all employees to change their access credentials and deployed additional endpoint protection on our corporate network to help prevent this type of incident from reoccurring in the future.

We are providing two years of free identity theft protection and credit monitoring services from a leading identity monitoring services company for individuals who opt in. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the enrollment instructions included with this letter.

What You Can Do

Although we are not aware of fraud arising from this incident, we want to make you aware of precautionary steps you can take:

- **Activating the Complimentary Identity Protection Services.** As outlined above, we are offering two years of free identity theft protection and credit monitoring services. For more information about these services and instructions on completing the enrollment process, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter. Note that you must complete the enrollment process by [DATE].
- **Checking Credit Reports and Financial Accounts.** You should carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed on the next page.

If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. You can also inform your state attorney general's office and the Federal Trade Commission ("FTC"). You can review your financial account statements to determine if there are any discrepancies or unusual activity. If you see discrepancies or unusual activity on your financial account statements, or see anything you do not understand, call the financial institution immediately.



- **Consulting the Identity Theft Protection Guide.** Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact us at 650-352-6650 between the hours of 9 AM to 5 PM Pacific time, Monday through Friday or via email at MCarusi@lightstonevc.com. Again, we sincerely regret any concern this incident may cause.

Sincerely,

Mike Carusi
Managing Director



Information about Identity Theft Protection

To help protect your identity, we are offering complimentary access to Experian's® IdentityWorksSM for two years.

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 at **[NUMBER]**. 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 this Identity Restoration support is available to you for **[TIMEFRAME]** 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 immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary two year membership.

This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **[DATE]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **[LINK]**
- Provide your **activation code**: **[CODE]**

Additional Details Regarding Your Two-Year 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.¹
- **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 ExtendCARETM**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance²**: Provides coverage for certain costs and unauthorized electronic fund transfers.

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² 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.



obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should 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 Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For additional information from the IRS about identity theft, please visit <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft> or call 800-908-4490. There may be similar resources available at the state level, and you can contact your state department of revenue directly for more information. A listing of state tax agencies' websites is available at <http://www.taxadmin.org/state-tax-agencies>.

For residents of Maryland: 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 residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/internet/privacy-and-identity-theft>.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from 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.ncdoj.gov.

For residents of the District of Columbia: You may also obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia: Office of the Attorney General for the District of Columbia, Office of Consumer Protection, 400 6th Street NW, Washington, D.C. 20001 202-442-9828, www.oag.dc.gov.

Security Freezes and Fraud Alerts: You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.



As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

For more information, including information about additional rights, you can visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>, <https://www.consumerfinance.gov/learnmore/>, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)

General Contact:

P.O. Box 740241, Atlanta, GA 30374
800-685-1111

Fraud Alerts and Security Freezes:

P.O. Box 740256, Atlanta, GA 30374

Experian (www.experian.com)

General Contact:

P.O. Box 2104, Allen, TX
75013

888-397-3742

Fraud Alerts and Security Freezes:

P.O. Box 9556, Allen, TX
75013

TransUnion

(www.transunion.com)

General Contact, Fraud Alerts and Security Freezes:

P.O. Box 2000, Chester, PA
19022
800-916-8800